Lov og nett

En kvantitativ studie av holdninger til personvern på internett

Dag Mostuen Grytli

Masteroppgave i medievitenskap

Institutt for medier og kommunikasjon

Det humanistiske fakultet

UNIVERSITETET I OSLO

[1.6.2015]

År: 2015

Tittel: Lov og nett. En kvantitativ studie av holdninger til personvern på internett

Forfatter: Dag Mostuen Grytli

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Sammendrag

Denne oppgaven undersøker sammenhengen mellom holdninger til personvern og de konkurrerende interessene sikkerhet og bekvemmelighet. I tillegg undersøker den hvilken betydning personlige negativer erfaringer med personopplysninger på avveie har for ønsket om lovregulering av flyten av personopplysninger på internett. Jeg har tatt utgangspunkt i et omfattende datamateriale samlet inn av Opinion Perduco, på oppdrag fra Datatilsynet. Dette har jeg analysert kvantitativt ved hjelp av krysstabellanalyser og bi- og multivariate regresjonsanalyser. Funnene viser at det ikke finnes noen sammenheng mellom overordnede holdninger til personvern og villighet til å ta i bruk personvernkrenkende teknologi. Samtidig har overordnede holdninger til personvern sammenheng med hvordan personvernet veies opp mot de konkurrerende interessene sikkerhet og bekvemmelighet, når disse er eksplisitt artikulert. Videre viser funnene at personlige erfaringer med uønsket bildepublisering og lav alder predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett. Utdanning og kjønn har ingen effekt på dette ønsket.

Abstract

This thesis examines the relationship between privacy attitudes and the competing interests of security and convenience. In addition, it explores the significance of personal, negative experiences when deciding what importance legal protection of the flow of personal information online should be given. The thesis uses an extensive data set, collected by Opinion Perduco, on behalf of the Norwegian Data Inspectorate. I have analyzed the data quantitatively, using crosstab analyzes and multivariate regression analyzes. The findings show that there is no correlation between overall privacy attitudes and willingness to use privacy infringing technology. Meanwhile, overall attitudes towards privacy correlates with how privacy is weighed against the competing values of security and convenience, when these are explicitly articulated. Furthermore, experiences relating to unwanted photo publishing predicates a stronger desire towards legal protection of the flow of personal information online. Younger people are also more inclined to welcome such protection. Sex and education does not have any such effect.

Forord

Først og fremst skylder jeg Audun Beyer en stor takk for hjelpen med denne oppgaven. Spesielt mot slutten av arbeidet har det vært enormt betryggende å ha en veileder som stiller opp på en slik måte som du har gjort. I tillegg vil jeg takke Anders Fagerjord for god veiledning i oppstarten av prosjektet. Catharina Nes i Datatilsynet fortjener også en stor takk for å ha gitt meg tilgang til datamaterialet jeg bygger oppgaven på. Håkon Henjum og Even Egeberg har også trådt til med råd og innspill, ofte på kort varsel. Mads Braarud og Bente Elnan har også bidratt med konstruktive tilbakemeldinger.

Alle jeg har delt denne siste innspurtstiden med på skrivestua på IMK bør også takkes. Norsk Kaffeinformasjon har gjennom hele mitt studieløp sørget for et akseptabelt koffeinnivå i blodomløpet. Antall studiepoeng fra IMK som delvis bør krediteres dem kan ikke overdrives.

Denne masteroppgaven mottok Fritt Ords studentstipend. Det har vært til stor hjelp i en ellers trang studentøkonomi.

Til sist vil jeg takke den viktigste personen i livet mitt, Synne. Ingen kjenner meg bedre, og ingen vet bedre enn deg når jeg trenger en kald øl og når jeg trenger å bli jaget ut i regnet på joggetur. Du har sørget for begge deler i løpet av denne tiden. Også Frida fortjener en takk for å hver eneste dag minne meg på at livet er så uendelig mye mer enn det som skjer på Blindern.

Oslo, juni 2015

Dag Mostuen Grytli

Innholdsfortegnelse

1 Innledning

To hendelser av svært ulik art, som fant sted sommeren 2013, oppsummerer hvorfor jeg valgte personvern på internett som tema for masteroppgaven min. Den første var Snowden-avsløringene, som avdekket amerikanske etterretningsmyndigheters kapasitet og vilje til å samle og lagre så mye informasjon som mulig om så mange som mulig. Private teknologiselskaper som Facebook, Google, Apple, Skype og Microsoft hadde gitt myndighetene tilgang til enorme mengder informasjon, og dermed demonstrert hvor tynn linjen mellom lovlig, kommersiell datainnsamling og ulovlig overvåkning er (Greenwald 2014, Gellman og Poitras 2013). Snowden avslørte blant annet at så å si alt vi gjør på internett registreres og analyseres, uten noen form for rettslig kjennelse (Greenwald 2013). Denne overvåkingspraksisen er blant annet basert på informasjon som disse selskapene samler inn i bytte mot gratis innhold og tjenester. Googles søkemotor er ikke gratis, du betaler for den med personopplysninger. Disse opplysningene er bestanddeler i et raskt voksende marked for personopplysninger. Jeg ble, i likhet med veldig mange, skremt av det Snowden avslørte. Jo mer jeg leste, jo mer sank det inn over meg hvor lite kontroll jeg har over den digitale informasjonen jeg med jevne mellomrom legger igjen på internett.

Samme sommer, ved en tilfeldighet, leste jeg boken *Big Data* av Viktor Mayer-Schönberger og Kenneth Cukier. Kort fortalt handler den om de enorme mulighetene som ligger i analyse av enorme datamengder, i alt fra sykdomsbekjempelse til effektive klimaløsninger. Disse mulighetene forutsetter enorme mengder digitalisert informasjon, og dermed er den samme teknologien potensielt et verktøy for uhyre effektiv overvåking, slik Snowden avslørte. Mye av denne informasjonen genereres automatisk i vår daglige interaksjon med digitale, nettverkstilknyttede medier.

Oppsummert førte disse to hendelsene, om enn vidt forskjellige i art og omfang, til en erkjennelse av at den teknologiske utviklingen – med internett som et særdeles viktig omdreiningspunkt – kan sies å representere et tveegget sverd. Skadepotensialet er stort, men det er også vinningspotensialet. Denne tosidigheten fremstår for meg som ekstremt viktig å anerkjenne i vår daglige omgang med ny teknologi. Selv om denne oppgaven fokuserer på noen av de problematiske sidene ved modellen dagens internett er basert på, vil jeg innledningsvis understreke at jeg på ingen måte underkjenner de uten tvil enorme potensielle gevinstene som eksisterer ettersom stadig mer sofistikert teknologi ser dagens lys. Med jevne

mellomrom – med Snowden-avsløringene som den mest dramatiske i nyere tid – får vi imidlertid påminnelser om hvilket skadepotensiale den samme teknologien bærer i seg. Tematikken er i tillegg i høyeste grad aktuell, og personvernets kår på internett er et felt hvor nye aspekter og perspektiver med jevne mellomrom entrer offentligheten. Schibsteds satsing på stordata for personalisert reklame (Brække 2015), og Facebooks arbeid med utbygging av internett i fattigere deler av verden, i bytte mot personinformasjon er bare noen, rykende ferske eksempler (Morozov 2015). I innspurten av arbeidet med masteroppgaven publiserte også Datatilsynet et innlegg på sin egen blogg, som omhandler mange av utfordringene jeg tar for meg i min oppgave (Nes 2015).

Mitt fokus vil hovedsakelig ikke være på de teknologiske aspektene ved internett. Et rent teknologisk perspektiv ville omhandlet nettverk, rutere, dataprogrammer og relaterte teknologiske komponenter som har muliggjort alt digitalt liv Å forstå internett som summen av alle disse komponentene reduserer internett til en uhyre sofistikert teknologisk vinning, men ikke så mye mer enn det. Mitt perspektiv er derimot det Helen Nissenbaum (2010, 4 – 6) skiller ut som det sosio-teknologiske perspektivet. Utviklingen av det vi i dag kjenner som internett har skjedd, og fortsetter å skje, i et uhyre komplekst samspill mellom sosiale, politiske, kulturelle og økonomiske prosesser, for å nevne noen, i likhet med hva som historisk har vært tilfelle med alle teknologiske nyvinninger. Når jeg videre i oppgaven benytter begrepet teknologi er denne brede forståelsen av begrepet viktig å ha i bakhodet.

1.1 Våre digitale fotavtrykk

Mennesker som lever i moderne samfunn ser til nettet for å løse stadig flere oppgaver, og stadig mer av interaksjonen mellom enkeltindivider og offentlige myndigheter, så vel som private selskaper, skjer på internett. Veldig lite tyder på at vi nærmer oss et endepunkt, der teknologien har maksimert sin nytteverdi. Eric Schmidt, direktør i Google, har uttalt at internett en gang vil bli borte, altså så sømløst integrert i alle handlinger at vi glemmer at det er der, slik vi i dag anser elektrisitet som en selvfølgelighet vi ikke tenker mye på (Smith 2015). PEW Research Centre publiserte i fjor resultatene av en stor ekspertundersøkelse med spådommer om internettet i 2025 (Anderson og Rainie 2014, 37). Blant hovedkonklusjonene var det sømløst integrerte nettet, som Schmidt snakker om. En annen var at «folk vil – om enn motvillig – fortsette å gjennomføre byttehandler som favoriserer bekvemmelighet og

umiddelbar vinning foran personvern» (Anderson og Rainie 2014, 11). Denne spådommen er utgangspunktet for min oppgave.

Verdier

Å leve digitale liv innebærer at vi etterlater oss digitale fotavtrykk, og disse informasjonsenhetene er potensielt veldig verdifulle for så vel offentlige myndigheter som private aktører. Personopplysninger registreres i økende grad og på stadig flere måter, og informasjonen lagres og analyseres ved hjelp av stadig mer sofistikerte verktøy. Informasjonsregistreringen er ofte automatisert, og skjer i tillegg ofte uten av den som avgir informasjonen er klar over det (REF). Informasjonen det er snakk innebefatter mye mer enn det brukergenererte innholdet ment for publisering, som bloggposter og informasjon i personlige nettsider. Også informasjon om søkehistorikk, hvilke nettsider man besøker, elektronisk betalingsinformasjon, lokasjonsdata fra GPS-sensorer og informasjon om interaksjon i sosiale nettsamfunn er en del av den enorme mengden informasjon vi genererer om oss selv når vi interagerer med nettverkstilknyttede, digitale medier (Andrejevic 2014, 50, Schartum og Bygrave 2011, 26).

Denne informasjonen er som nevnt veldig verdifull. Internett baserer seg i stor grad på en modell som forutsetter at brukeren gir fra seg personopplysninger i bytte mot gratis tjenester og informasjon (Shapiro 1999, 160, Andrejevic 2014, 92 – 97, Papacharissi 2010a). Denne byttehandelen, koblet med stadig bedre prosesseringskraft og nær ubegrensede lagringsmuligheter, har muliggjort fremveksten av et enormt marked for kjøp og salg av digitaliserte personopplysninger. Vi er ofte velvillige, og også ofte uvitende, selgere av denne informasjonen, gjennom stadig mer aktiv digital tilstedeværelse. Søkehistorikk lagres av Google, internettsider registrerer ditt digitale bevegelsesmønster og Facebook tjener enorme pengesummer på å selge informasjon om «like»-historikken din. I stedet for et månedlig beløp trukket fra bankkontoen din trekker disse selskapene verdier ut av informasjonen den digitale aktiviteten genererer. Dette markedet, der internettbrukere «betaler» for tjenester og innhold med personopplysninger er problematisk av en rekke grunner, og felles for disse er at de legger press på personvernet i vår digitale tidsalder.

Det er imidlertid viktig å påpeke at i mange tilfeller er denne registreringen en indirekte konsekvens av en annen funksjon teknologien er ment å fylle (Nissenbaum 2010, 24). Betaling med kredittkort er for eksempel enklere, raskere og mye tryggere enn betaling med

kontanter, men dette systemet forutsetter at alle transaksjoner registreres. David Lyon (2001, 16) hevder at den stadig tiltakende graden av registrering bør forstås som en konsekvens av historiske og sosiale endringsprosesser som har muliggjort det han kaller «the disappearing bodies». Det moderne samfunnets integrasjonsmåter har radikalt endret seg som følge av at endrede transport- og kommunikasjonsmåter har ført til at den fysiske tilstedeværelsen ikke lenger er avgjørende for sosial integrasjon. Dermed forstås den stadige registreringen av personopplysninger som det moderne samfunnets substitutt for tidligere historiske epokers tillitsmarkører, som fysiske kropper, øyekontakt og håndtrykk. Hvis du ikke har betjent kredittkortgjelden din vil det gå ut over din troverdighet og medføre at du ikke får ta opp lån, og dermed er registreringen av transaksjoner med betalingskortet en tillitsmarkør for din troverdighet.

Registrering på flere måter

Nettsurfing, bruk av søkemotorer og elektronisk betaling er bare noen av handlingene som etterlater seg et digitalt fotavtrykk, informasjon om ditt digitale handlingsmønster. I dag har også smarttelefonens utbredelse sørget for at de samme verktøyene som for noen år siden var fysisk stedbundne til datamaskinen hjemme, bæres rundt i lommer og vesker. Dermed har også bevegelsesmønstre i den fysiske verden blitt inkorporert i den stadig voksende informasjonsmengden som eksisterer, muliggjort gjennom lokasjonsdata som genereres ved hjelp av GPS-teknologi. Denne teknologien muliggjør for eksempel at nærmeste bussholdeplass dukker opp automatisk i en installert app når du skal reise et sted. Kollektivtrafikkselskaper, som Ruter, benytter på sin side informasjon fra alle som benytter appen deres til å fastslå hvor det behøves flere bussavganger i bestemte tidsperioder, altså har informasjonen stor nytteverdi for å skape mer effektiv kollektivtrafikk. Den samme informasjonen har imidlertid også et enormt potensiale som overvåkingsverktøy, og gjør – i kombinasjon med de stadig mer allestedsværende overvåkningskameraene – at anonymitet i det offentlige rom blir vanskeligere, i det minste i byene.

Smarttelefonene, som de siste årene har blitt allemannseie, er i tillegg til disse funksjonene også som regel utstyrt med ulike sensorer som kan kartlegge kroppslige egenskaper som søvnmønster, hjerterytme, kroppstemperatur og puls. Igjen er det viktig å understreke hvordan denne utviklingen både har et vinnings- og et skadepotensiale. Systematiske kartlegging av søvnmønster kan utvilsomt hjelpe mennesker til å hanskes med eventuelle søvnproblemer,

ved å opplyse om søvnsykluser og ideelle oppvåkningsfaser. Jevnlige målinger av puls og hjerterytme kan bidra til å avdekke helsemessige faresignaler, og være et verktøy for bedre helse og livskvalitet. På den annen side kan en systematisk kartlegging av søvnmønster og puls være verdifull informasjon for forsikringsselskaper som skal avgjøre hvor vidt du kvalifiserer til å tegne livsforsikring. En arbeidsgiver vil på lignende vis sannsynligvis være mer tilbøyelig til å ansette en person med gode søvnvaner og lav hvilepuls – begge objektive tegn på god helse. Lovverket forhindrer at forsikringsselskaper og arbeidsgivere har tilgang til legejournaler som forteller om eventuelle søvn- og hjerteproblemer. Når den samme informasjonen eksisterer i privateide databaser i USA, fordi du selv har kartlagt den, er ikke denne beskyttelsen like sterk.

Mye av informasjonen som genereres av våre digitale fotavtrykk oppstår som følge av at vi i så stor grad interagerer med nettverkstilknyttede digitale medier. Veldig mange av disse er i tillegg privateide selskaper, med Google og Facebook som de aller største. Informasjonen som genereres lagres på enorme servere i USA og siden lagringskapasiteten har økt og kostnadene sunket, vil det alltid være mer hensiktsmessig for disse selskapene å beholde dataene enn å slette dem (Mayer-Schönberger og Cukier 2013, 100 – 101). Denne økonomiske kalkylen gjør at det bygges enorme dataregistre om alle mennesker som benytter slike tjenester, og disse dataregistrene eksisterer både fysisk og juridisk utenfor enkeltindividenes rekkevidde.

Å kjøpe en pizza – et eksempel

Når du taster inn ordet «pizzarestaurant Oslo» i Googles søkemotor på smarttelefonen din registreres dette søket automatisk, samtidig som du, helt gratis, får informasjon om et enormt antall muligheter for å stilne hungeren etter pizza i byen du befinner deg i. Ifølge Wikipedia (2015) gjennomføres det omtrent tre milliarder googlesøk per dag, noe som innebærer at dette selskapet har enorm detaljkunnskap om hva mennesker over hele verden søker informasjon om, inkludert hvor det oftest letes opp informasjon om pizzarestauranter i Norges hovedstad. Når du så har valgt deg ut et pizzasted, tatt bussen tre holdeplasser mot sentrum og bestilt en stor pepperonipizza til å ta med hjem, er sannsynlighet stor for at du betaler med bankkort. Igjen registreres det at du har betalt et beløp i størrelsesordenen 200 kroner til pizzarestauranten. I sum har du ved hjelp av ulike digitale verktøy på en effektiv måte oppnådd det umiddelbare målet om tilfredsstillelse av den gnagende pizzasulten.

Det er imidlertid én viktig feil ved redegjørelsen ovenfor. Informasjonen du har tatt i bruk for å oppnå målet er ikke gitt deg gratis. Du betaler riktig nok ikke for den i kroner og øre, men gjennom en byttehandel, der tjenestetilbyderen – Google, Ruter og banken din i eksempelet ovenfor – lagrer informasjonen om den digitale aktiviteten din for fremtidig bruk, analyser og videresalg. Denne informasjonen kan benyttes til mye. Som nevnt kan Ruter la informasjonen inngå i det store logistiske regnestykket som gjør at kollektivtrafikken i Oslo flyter best mulig. Banken din kan analysere kjøpsvanene dine og finne ut om du egentlig kunne klart deg med et vanlig bankkort i stedet for det dyre kredittkortet du bruker i dag. Og endelig kan Google selge informasjonen de sitter på – generert blant annet av 3 milliarder søk hver eneste dag – til annonsører som ønsker mer valuta for pengene de bruker ved hjelp av målrettet reklame. Dermed er det sannsynlig at det neste gang du tar frem smarttelefonen et sted i Oslo sentrum, dukker opp reklame for en pizzarestaurant i nærheten.

1.2 Problemer

Eksempelet ovenfor kan fremstå som rimelig uskyldig. Det kan også argumenteres for at en slik utvikling er positiv. Man blir uansett eksponert for reklame hver eneste dag, så hvorfor ikke tillate at reklamen blir personalisert? Er man glad i pizza kan det føles meningsløst å få stadige påminnelser om alle vegetarianerrestaurantene i byen. Målrettet reklame er likevel bare ett eksempel på hvordan dine digitale fotavtrykk settes i arbeid for å generere profitt. Dagens internett baserer seg i stor grad på en slik modell, som innebærer at innhold og tjenester tilbys gratis i bytte mot personlig informasjon (Shapiro 1999, 160, Andrejevic 2014, 92 – 97, Papacharissi 2010a). Tjenestene Google tilbyr koster ikke noe i kroner og øre, men selskapet samler inn, lagrer og selger personinformasjon om deg til tredjeparter, i tillegg til at informasjonen benyttes til å forbedre Googles egne tjenester. Den enorme mengden informasjon disse selskapene sitter på muliggjør analyser av kjøpsvaner, søkehistorikk, nettsidebesøk og bevegelsesmønstre ved hjelp av lokasjonsdata. På samme måte innebærer å ha en Facebook-konto en aksept av å inngå i en byttehandel med selskapet. Du får tjenesten, Facebook får informasjon om blant annet ditt personlige nettverk og smakspreferanser, gjennom din «like»-historikk. Selv om selskapene anonymiserer informasjon før videre salg er det flere problemer som hefter ved denne praksisen.

Overvåking

For det første representerer denne informasjonen en gullgruve for politi og etterretningstjenester, og noe av det Edward Snowden avdekket var at NSA har hatt tilgang på denne gullgruven lenge (Gellman and Poitras 2013). I tillegg til informasjonen som genereres når vi benytter digitale verktøy hadde samme etterretningsorganisasjon tilgang på store mengder privat kommunikasjon i form av email og meldinger i sosiale nettsamfunn, igjen registrert og lagret av private internettselskaper. Overvåkningen av privat kommunikasjon – en overvåkning som til og med rammet Europas mektigste politiske leder, Tysklands forbundskansler Angela Merkel (Pengelly 2014) – vil imidlertid ikke være mitt hovedfokus, men det er viktig å nevne for å understreke omfanget av avsløringene. Det tjener også som en påminnelse om at skottene mellom selskapene som samler informasjon og myndigheter som ønsker tilgang på disse på langt nær er tette, selv når informasjonen i utgangspunktet er høyst privat kommunikasjon.

De samme etterretningsorganisasjonene kan, ved hjelp av stadig mer sofistikerte analysemetoder, re-identifisere individer ved hjelp av sammenstilling av i utgangspunktet anonymisert informasjon. To journalister demonstrerte hvordan slik re-identifisering kan gjøres. Ved hjelp av en sammenstilling av søkehistorikk offentliggjort av internettleverandøren AOL klarte de å re-identifisere bruker nummer 4417749 som 62 år gamle Thelma Arnold (Barbaro 2006). Internettselskapenes lovnader om at personidentifiserende informasjon fjernes før videre bruk er med andre ord ikke nødvendigvis noen sikker garanti for at du forblir anonym.

Problemer i markedet

Det andre problemet, som vil bli denne oppgavens hovedfokus, omhandler selve byttehandelen, der brukere får tilgang på tjenester og innhold i bytte mot personinformasjon. Flere undersøkelser har vist at internettbrukere ikke forstår i hvilket omfang personopplysningene settes i bruk, kjøpes og selges mellom kommersielle aktører (Turow, Mulligan og Hoofnagle 2007, Hoofnagle og King 2008, Turow 2003, 19). Maktforholdet mellom tjenestetilbydere og brukere er i tillegg skjevt, og selskapene har ofte interesse av å ikke oppgi optimal informasjon om implikasjonene av å ta i bruk en tjeneste (Schwartz 1999, 1684). Kontraktene internettbrukere godtar idet en tjeneste tas i bruk er følgelig også utformet i lite brukervennlig språk, og fungerer ofte som juridisk beskyttelse for selskapene snarere enn

god brukerveiledning (Solove 2004, Pollach 2007, Papacharissi og Fernback 2005). I tillegg er det problematisk at verdien av personopplysningene som brukeren avgir umulig kan fastsettes på tidspunktet for avtaleinngåelsen, fordi den potensielt store gevinsten ligger langt frem i tid, når en stor mengde informasjon sammenstilles (Solove 2004, 87 – 88, Froomkin 2000, 1502 – 1503). Det er også tvilsomt om byttehandelen kan sies å være rettferdig når alternativet til å ikke godta selskapenes vilkår innebærer tilbaketrekning fra digitale fora, noe som for de færreste er et reelt alternativ (Lüders 2008, 104 – 105). Endelig er det grunn til å tro at dette markedet kan skape et personvernskille på nett, hvor kun ressurssterke individer makter å ivareta sitt eget personvern (Papacharissi 2010).

1.3 Personvern

Selv om det er stor forskjell på ulovlig overvåkning av privat kommunikasjon og personalisert reklame basert på registrerte opplysninger om digital atferd, er fellesnevneren at begge deler legger press på personvernet. Alle utfordringene knyttet til markedet for personopplysninger på nett som jeg så langt har redegjort for er personvernutfordringer. Begrepet *personvern* lar seg ikke med letthet definere, og har alltid vært preget av terminologisk uklarhet, forvirring og strid (NOU 2009:1, 29). Et kapittel i teoridelen vies derfor til en drøfting av dette begrepet, samt det relaterte engelske begrepet *privacy*. Til tross for denne begrepsmessige forvirringen er det like fullt personvernet som ligger i potten når vi bytter personopplysninger mot tjenester og innhold på internett.

Personvernparadokset

Flere undersøkelser har vist at folks uttalte bekymring for personvernets kår er sterk – og tiltakende. Hele ni av ti oppgir for eksempel å være svært eller ganske opptatt av personvern i Datatilsynets undersøkelse (Datatilsynet 2013). I tillegg oppgir 45 % i samme undersøkelse at de er blitt *mer opptatt* av personvern de siste to, tre årene. Denne bekymringen er også ofte knyttet til mangelen på kontroll over personopplysninger på internett. Det er imidlertid lite som tyder på et grasrotopprør mot denne praksisen. Personvernbevisste individer opptrer ikke som personvernbevisste forbrukere på internett. Flere undersøkelser peker i retning av at de fleste av oss gladelig avgir informasjon i bytte mot gratis tjenester på internett, til tross for sterk uttalt bekymring for personvernet (Fox et al. 2000, Nissenbaum 2010, 104). Dette har fått merkelappen *personvernparadokset* (Barnes 2006, Norberg, Horne og Horne 2007, 101).

Vi postulerer viktigheten av et godt personvern i samme åndedrag som vi godtar at personopplysninger registreres i databaser på andre siden av jorden. Det er imidlertid tungtveiende grunner til at en slik tolkning bør nyanseres. Disse vil drøftes i siste del av teorikapittelet.

Personvern er som jeg vil redegjøre for i neste kapittel, et vanskelig og mangefasettert konsept. Det er likevel liten tvil om at beskyttelse av individets integritet, kommunikasjon og informasjon er et ønskelig ideal, og noe som anses som viktig. Det er også et faktum at disse idealene konstant presses, veies mot andre hensyn og utfordres blant annet av statlige og private institusjoner og organisasjoner som kan ha interesse av et svakere personvern. Motivasjonen for disse vil samtidig variere kraftig, fra legitime interessemotsetninger som personvern kontra effektiv kriminalitetsbekjempelse til rene økonomiske kalkyler om effektiv, personalisert annonsering. Slike konflikter, mellom personvern og konkurrerende interesser, oppsto på ingen måte med introduksjonen av internett og vår tids digitale tilstedeværelse. Pressens eldgamle og pågående kamp for et trygt kildevern er et eksempel på en lignende interessekonflikt.

Interesseavveiinger

Interessemotsetningen mellom personvern og sikkerhet var en hoveddrivkraft bak overvåkingspraksisen som Snowden avslørte. I kjølvannet av terrorangrepene 11. september fikk amerikansk etterretning videre overvåkningsfullmakter for å forhindre et lignende anslag, gjennom den kontroversielle USA Patriot ACT[1]. Det er imidlertid viktig å understreke at det ikke finnes noe fasitsvar på hvor balansegangen mellom hvilke fullmakter politi og etterretning skal ha i sitt arbeid for å bekjempe kriminalitet og borgernes personvernrettigheter går. Konstante interesseavveiinger er en uunngåelig del av å leve i et åpent, pluralistisk samfunn (Nissenbaum 2010, 110), og et sentralt kjennetegn ved disse er at interessene som veies opp mot hverandre ofte er svært ulike (Schartum og Bygrave 2011, 44).

I vår daglige interaksjon med digital teknologi er det imidlertid en annen interessemotsetning som er sentral. Samtlige av de teknologiske verktøyene som ble benyttet av personen som skulle stilne pizzasulten bidro til at oppgaven ble løst mer *effektivt* og sørget for økt

[1] USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Electronic Frontier Foundation). Særdeles omfattende lov som gir amerikanske etterretningsmyndigheter vide overvåkingsfullmakter for å bekjempe terrorisme.

bekvemmelighet. Det samme oppdraget – finne en pizzarestaurant, komme seg dit og betale – ville vært mye mer tidkrevende og strevsomt uten de elektroniske hjelpemidlene. Listen over teknologi som har økt effektiviteten og bekvemmeligheten i dagens informasjonssamfunn er lang, fra epost som muliggjør global kommunikasjon på et tidels sekund til automatiske bomstasjoner, som sørger for at trafikken flyter, og du slipper å huske på å ha mynter i hanskerommet. En forutsetning for alle disse er imidlertid at informasjon registreres. Teknologisk utvikling spiller altså en nøkkelrolle i slike interessekonflikter, og vi lever i en tid hvor denne utviklingen skjer i et heseblesende tempo.

1.4 Problemstillinger

På bakgrunn av redegjørelsen ovenfor har jeg formulert to hovedproblemstillinger, som jeg vil undersøke ved hjelp av to separate analysedeler. Den første analysen tar sikte på å undersøke sammenhengen mellom ulike mål på holdninger til personvern, i lys av tidligere undersøkelser og teori. Hovedfokus for denne analysedelen vil være hvordan personvern vurderes opp mot konkurrerende interesser. Den første problemstillingen vil derfor være:

Finnes det en sammenheng mellom hvor opptatt man er av personvern og

a) Hvor villig man er til å ta i bruk personvernkrenkende teknologi?

b) Hvordan man veier personvernet opp mot andre interesser på et overordnet nivå?

Den første analysedelen tar altså sikte på å undersøke hvordan overordnede holdninger til personvern samsvarer med villighet til å benytte teknologi som krenker personvernet, og også hvordan overordnede holdninger til personvern vurderes opp mot to interesser som personvern ofte veies opp mot, *sikkerhet* og *bekvemmelighet*, når disse er eksplisitt artikulert.

I den andre analysen vil jeg forsøke å gå ett steg videre. På bakgrunn av funn og teori som peker på ulike problemer i markedet for personopplysninger, vil jeg undersøke om personlige, negative erfaringer med tap av kontroll over personopplysninger innebærer endrede holdninger til personvern. Det er nemlig, som jeg vil redegjøre for i teorikapittelet, tungtveiende grunner til at internettbrukere som er opptatt av eget personvern ikke kan ivareta dette slik dagens internett fungerer. Likevel er det forbundet risiko med å stadig etterlate seg digitale spor i samhandling med nettverkstilknyttede digitale medier. Det er derfor grunn til å

tro at personlige, negative erfaringer kan føre til at de overordnede holdningene til personvern endres. Den andre problemstillingen vil følgelig bli:

Predikerer personlige negative erfaringer med tap av kontroll over personopplysninger et sterkere ønske om lovregulering av flyten av personopplysninger på nett?

Denne oppgaven baserer seg på data samlet inn av analyseselskapet Opinion Perduco, på oppdrag av Datatilsynet. Datamaterialet ble brukt i arbeidet med *Personvernundersøkelsen 2013/2014.* Jeg vil diskutere fordeler og ulemper ved denne måten å løse oppgaven på i metodekapittelet. Spørsmålene fra spørreskjemaet som jeg benytter i analysene kan finnes som vedlegg 1.

1.5 Gang i oppgaven

Denne oppgaven består av seks deler, inkludert innledningskapittelet. Jeg vil begynne med en konseptuell redegjørelse av personvernbegrepet, og et forsøk på å forklare hvorfor personvernteori preges av konseptuell uenighet og strid (2). Jeg vil redegjøre for ulike måter å forstå personvernbegrepet på, og forklare hvorfor begrepet *personopplysningsvern* i moderne tid har blitt skilt ut som en sentral kategori. Videre følger et kapittel jeg har kalt personopplysninger til salgs (3). Her vil jeg peke på og diskutere ulike grunner til at individet stiller svakt i møte med tjenestetilbydere på nett. Dette markedet preges blant annet av et veldig skjevt maktforhold, utstrakt kunnskapsmangel og ikke-fungerende kontrakter, noe som i sum gjør at byttehandelen internettbrukere inngår med tjenestetilbydere på nett på langt nær kan kalles rettferdig og meningsfull. Videre vil jeg argumentere for at det ikke kan sies å være et paradoks at personvernbevisste mennesker ikke opptrer som personvernbevisste forbrukere, slik dagens internettmodell er, på grunn av disse markedsproblemene. Jeg vil avslutte med å forklare hvordan Snowden-avsløringene kan sies å ha avdekket sammenkoblingen mellom tilsynelatende uskyldig registrering av personopplysninger og ulovlig overvåkning. Etter dette følger et metodekapittel (4), hvor jeg redegjør for det metodiske opplegget oppgavens analyser bygger på. Jeg vil ta for meg og drøfte variablene som inngår i analysen, samt analyseteknikkene jeg har valgt å ta i bruk. Kapittelet avsluttes med en diskusjon av begrepene reliabilitet, validitet og generaliserbarhet. Så følger en analysedel (5), hvor funn blir presentert og diskutert. Jeg vil begynne med å utforske om det finnes en sammenheng mellom overordnede personvernholdninger og villighet til å benytte personverntruende

teknologi. Videre vil jeg undersøke sammenhengen mellom personvernholdninger på et overordnet nivå med hvordan personvernet veies opp mot konkurrerende interesser. Siste analysedel tar sikte på å undersøke om personlige negative erfaringer med tap av kontroll over personopplysninger predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett. Til sist vil jeg diskutere funnene fra de to analysedelene opp mot hverandre og de teoretiske perspektivene i et avsluttende diskusjonskapittel (6). I tillegg inkluderer dette kapittelet en diskusjon av oppgavens begrensninger, videre forskning, samt en kort diskusjon av oppgavens reliabilitet og validitet.

2 Personvern

> Privacy, privacy, the new American obsession: espoused as the most fundamental of rights, marketed as the most desirable of commodities, and pronounced dead twice a week (Jonathan Franzen, Imperial Bedroom, 2010).

Sitatet over fanger etter min mening opp to tilbakevendende aspekter ved diskusjoner om personvern: For det første at personvern er et begrep som ikke med enkelthet lar seg definere. Jeg vil derfor bruke noe plass på å redegjøre for ulike teoretiske definisjoner, både fra norsk og internasjonal litteratur. For det andre er det sterke språket en indikasjon på at det er et veldig verdiladet begrep. Sammenstilt kan vi dermed hevde at mye diskusjon om personvern har et paradoksalt utgangspunkt: Personvern er ønskelig, beskyttelsesverdig og verdiladet, samtidig som begrepet er mangefasettert og vanskelig å definere.

Personvernutvalget, som i 2009 avga rapporten *Individ og Integritet*, understreker på lignende vis at «[d]iskursen rundt personvernbegrepet har alltid vært preget av terminologisk uklarhet, forvirring og strid» (NOU 2009:1, 29). Samme rapport slår også fast at begrepet – uansett definisjon – er et særnorsk begrep. Et vidt favnende forsøk på å etablere en definisjon kan finnes i *Data og personvern* (Selmer og Blekeli 1977, 13): «Personvern kan i utgangspunktet sees som en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem». Denne definisjonen, skrevet på et tidspunkt hvor den norske betegnelsen *personvern* var kun få år gammel (Selmer og Blekeli 1977, 13), ble i tiden som fulgte adaptert og akseptert både i offentlige organer som Datatilsynet og i den offentlige debatten generelt .

En slik definisjon ligger tett opp mot Alan Westins utgangspunkt for boken *Privacy and Freedom* (1967), som regnes som utgangspunktet for det moderne personvernet, da personvernproblematikk eksplisitt ble knyttet til frykten for hvilken makt som lå i at opplysninger om enkeltindivider ble lagret i stadig større dataregistre (Westin 1967, 158). Dette vil bli hovedfokus i del 3 av dette kapittelet.

2.1 Begrepet *privacy*

På liknende vis er det beslektede, engelske begrepet «privacy» et notorisk ambiguøst begrep, som kan oversettes til norsk på flere forskjellige måter, alle med ulikt meningsinnhold. Kunnskapsforlagets engelske ordbok (1996) oppgir fire ulike oversettelser:

> (1) uforstyrrethet; **in the privacy of your own home;** (2) privatliv (3) **in the strictest privacy** i den største hemmelighet og (4) **protection of privacy;** personvern.

De fire definisjonene spriker altså merkbart i meningsinnhold, og illustrerer på mange måter hvorfor begrepet er såpass uhåndgripelig. Det er for eksempel åpenbart stor forskjell mellom å forstå *privacy* som hemmelighold og uforstyrrethet. Lee A. Bygrave (2002, 128 – 129) drøfter i boken *Data Protection Law* «privacy»-begrepet, og fremsetter fire ulike måter å definere konseptet på. En lignende inndeling kan finnes i Solove (2008, 14 – 37) , med to kategorier Bygrave ikke har inkludert. Den første kategorien definisjoner anser begrepet for å relatere til uforstyrrethet – *non-interference* – som også er ordbokens første definisjon av begrepet. En slik forståelse av *privacy* kan spores tilbake til Samuel Warren og Louis Brandeis' essay *The Right to Privacy* (1890), som omtales som fundamentet for personvernlovgivning i USA (for eksempel Solove 2008, 15). Et slikt syn på «privacy»-begrepet tar utgangspunkt i enkeltindividet som ukrenkelig, og definerer «privacy»-begrepet som «retten til selv å velge i hvilken grad ens tanker og følelser skal kommuniseres til andre» (Solove 2008, 16).

Den neste gruppen definisjoner definerer begrepet i form av graden av tilgang til personen – *limited access to the self*. En slik forståelse er nært forbundet med den første (Bygrave 2002, 128, Solove 2008, 18), og kan forstås som en mer sofistikert formulering av uforstyrrethet. Forskjellen med de to er at sistnevnte kategori også anerkjenner at individet er en del av en større enhet – samfunnet – og at individet har rett til å begrense myndigheters og andre aktørers tilgang. Konseptet *limited access to the self* er altså en definisjon som forstår privacy som noe mer enn retten til å være alene (Solove 2008, 19).

Den tredje definisjonsgrupperingen forstår «privacy»-begrepet som informasjonskontroll, altså den fjerde definisjonen fra ordboken. Denne definisjonens mest innflytelsesrike talsmann er nevnte Alan Westin, som allerede i 1967 skrev at «[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others» (1967, 7). Som nevnt er det denne definisjonen som har vunnet frem som den dominerende i norsk debatt om personvern, og en slik forståelse ligger tett opp mot Blekelis definisjon. Denne kategorien personvern er følgelig også denne oppgavens fokus, og vil bli grundigere diskutert i et eget kapittel.

En fjerde gruppering relaterer «privacy»-begrepet til aspektene ved en persons liv som anses som *intime* eller *sensitive*, og relaterer dermed til den tredje ordboksdefinisjonen. Ifølge en slik forståelse vil det kun være avsløring av sensitive opplysninger som medfølger et tap av *privacy.*

I tillegg til disse fire kategoriene har Daniel Solove inkludert kategoriene *secrecy*, altså hemmelighold og *personhood.* Førstnevnte begrep beskrives som en underkategori av begrenset tilgang-teorien, men med et enda mer ensidig fokus på individets mulighet til å holde informasjon skjult (Solove 2008, 22). Begrepet *personhood*, som ikke med enkelthet lar seg oversette til norsk, relaterer i Soloves redegjørelse til en videreføring av Warren og Brandeis' teori, nærmere bestemt formulering om det ukrenkelige individ. Denne kategorien skiller seg fra de andre da den har et normativt utgangspunkt, og dermed tar utgangspunkt i at *privacy* er et mål i seg selv, da det hegner om individets ukrenkelighet (Solove 2008, 30).

2.2 Det moderne personvernet – fra personvern til personopplysningsvern

Det er altså mange og til dels motstridende måter å definere begrepet personvern, samt det engelske begrepet *privacy* på. Definisjonen som har vunnet frem som dominerende i norsk personverndebatt, personvern som informasjonskontroll, er denne oppgavens hovedfokus. Schartum og Bygrave (2011, 25) skriver at «det "moderne personvernet" fra og med 1970-årene var knyttet til datamaskinbehandling av personopplysninger i "registre"». Denne sammenkoblingen var utgangspunktet for Alan Westins *Privacy and Freedom* (1967), som trekkes frem som et pionerverk innen personvernproblematikk knyttet til personopplysninger.

> The issue of privacy raised by computerization is whether the increased collection and processing of information for diverse public and private purposes, if not carefully controlled, could lead to a sweeping power of surveillance over individual lives and organizational activity (Westin 1967, 158).

Solove (2008, 24) begynner diskusjonen av underkategorien *kontroll over personopplysninger* med denne boken, i likhet med Selmer og Blekeli (1977, 16). Bekymringen var altså fundert i de mange og kraftige mulighetene som lå i å samkjøre, søke gjennom, utveksle og manipulere de digitale «registrene» som inneholdt personopplysninger om enkeltindivider. Siden Westin skrev disse ordene for nesten femti år siden, har imidlertid den teknologiske utviklingen fundamentalt forandret mengden informasjon som eksisterer, samt mulighetene til å utnytte

den. I tillegg registreres langt mer informasjon automatisk, og informasjonen innebefatter mye mer enn skrift og tegn, som var tilfelle for femti år siden. I dag er også lyd og bilde en del av det digitale fotavtrykkene vi etterlater oss i vår interaksjon med digitale medier (Schartum og Bygrave 2011, 25 – 26).

Personopplysningsvern som selvstendig kategori

Personvernkommisjonen tok i 2009 til orde for et formelt skille mellom *personvern* på den ene siden og *personopplysningsvern* på den andre, et skille som ifølge kommisjonen allerede benyttes innen EU. Personvern forstås dermed som «ivaretakelse av personlig integritet, ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse» Personopplysningsvern på den annen side dreier seg om:

> Regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold (NOU 2009:1, 32).

Et slikt skille innebærer altså at *personopplysningsvern* forstås som «regler og standarder (…) som har ivaretakelse av personvern som hovedmål». Personvernkommisjonen skiller altså ut *informasjonskontroll* (Bygrave 2002: 128 – 129, Solove 2008: 24) som en hovedkategori innen personvernproblematikk, med de andre kategoriene – privatliv, selvbestemmelse (autonomi) og selvutfoldelse – som det overordnede målet. Man kan dermed hevde at Personvernkommisjonen formelt har adaptert Westins syn på personvern som kontroll over personopplysninger som en underkategori innen personvernproblematikk så sentral at den bør stå alene.

Schartum og Bygrave (2011, 32) beskriver på samme måte personopplysningsvern som en egen klasse personvernspørsmål, forbundet med bruken av IKT, men like fullt nært forbundet med de tradisjonelle personvernspørsmålene. På samme måte skiller Frederick Schauer (1998, 555) ut *database privacy* som «the purported right of individuals to control the distribution and the availability of information about themselves that may appear in various governmental and non-governmental databases», Denne definisjonen av personvern vil som nevnt være mitt fokus. Når jeg videre i oppgaven snakker om *personvern* vil det være det moderne

personvernet, forstått som personopplysningsvern jeg refererer til, med mindre noe annet er presisert.

2.3 Personvern på ulike nivåer – fra ideal til konkrete tiltak

Schartum og Bygrave (2011, 36 – 37) skriver at uenigheten blant forfattere omkring hva personvern *er,* blant annet dreier seg om «hvorvidt personvern betegner interesser, verdier, normer eller en tilstand». Videre forsøker de å løse den definisjonsmessige utfordringen som ligger i personvernbegrepet med å fremstille de ulike aspektene som «et hierarki der flere av de nevnte begrepene inngår, dvs. på flere sammenhengende nivåer» (Schartum og Bygrave 2011, 37). På det øverste nivået fremstilles personvern som et *ideal,* altså en rendyrket tilstand vi streber mot. Denne ideelle tilstanden kan imidlertid ifølge forfatterne ikke oppfylles fullt ut, av to grunner. For det første vil personvernet komme i konflikt med andre idealer, og det vil oppstå behov for avveininger. Dette kan oppstå når personvernidealet kolliderer med ytringsfrihetsidealet, eksempelvis pressens legitime rett til å undersøke en offentlig persons økonomiske forhold. For det andre vil det av praktiske årsaker være umulig å sette et slikt ideelt personvernregime i live, da menneskelig og teknisk svikt sannsynligvis vil hindre at et slikt regime vil fungere (Schartum og Bygrave 2011, 37). På det neste nivået finner vi *personverninteresser*, «de sider ved personvernidealet som klart er synliggjort og dermed aktualisert i vårt samfunn» (Schartum og Bygrave 2011, 38). Interesseteorien, som jeg vil redegjøre for i det neste avsnittet, angir slike personinteresser. Videre angis et lag av *personvernkrav*, som en konkretisering av interessene, og til sist et lag av *personverntiltak,* som begrunnes i personvernkravene.

2.4 Interesseteorien

Schartum og Bygrave (2011, 41) presenterer *interesseteorien* som «den katalogen av personverninteresser som har vært utviklet gjennom de siste 30 år». Forfatterne formulerer videre fem ulike interesser, som i sin tur elaboreres i spesifikke krav, i tråd med overnevnte nivådeling. Disse fem er (1) Interessen i å bestemme over tilgangen til opplysninger om egen person, (2) interessen i innsyn og kunnskap, (3) interessen i opplysning- og behandlingskvalitet, (4) interessen i forholdsmessig kontroll og (5) interessen i brukervennlig behandling (Schartum og Bygrave 2011, 46 – 80). Det er ikke hensiktsmessig, eller mulig å

redegjøre detaljert for samtlige av disse interessene, eller de 18 kravene som følger av de. Det er imidlertid viktig å peke på at en slik forståelse knytter personvern til konkrete beslutningsprosesser (Bygrave 2002, 140, Blekeli 1977, 21 – 23). Det er også verdt å merke seg at Schartum og Bygraves oppsummering av personverninteressene til en viss grad skiller seg fra tidligere litteratur på området. Bygrave (2002, 140) skriver for eksempel at «tre hovedinteresser har vært knyttet til personvern. Oppsummert er disse interessene formulert som diskresjon, innsyn og fullstendighet» (min oversettelse). Den samme oppsummeringen finner vi i Blekeli (1977, 23 – 24). Det er imidlertid ikke snakk om et brudd med tidligere tenkning, men snarere en supplering og videreføring av tradisjonelle bidrag på personvernfeltet (Schartum og Bygrave 2004, 41).

Som tidligere nevnt er det viktig å notere at disse personverninteressene ikke er enerådende (Schartum og Bygrave 2011, 43), men må avveies mot andre interesser. Schartum og Bygrave (2011, 43) skiller mellom *individuelle* og *generelle* interesseavveiinger. En individuell interesseavveining på vil for eksempel oppstå når man må veie verdien av en gratis emailtjeneste, som muliggjør effektiv kommunikasjon, mot personverntapet som følger av å avgi opplysningene. Politiske myndigheters avveining mellom sikkerhet og personvern er et klassisk eksempel på en generell interesseavveiing. Det er imidlertid viktig å huske på at slike interessekonflikter er uunngåelig i et pluralistisk samfunn. Det er også et karakteristisk trekk ved slike avveiinger at «de interesser som skal vurderes opp mot hverandre, ofte er av vidt ulik karakter» (Schartum og Bygrave 2011, 44).

2.5 Kontekstuell integritet

Personvern, herunder også de ulike tolkningene av det engelske *privacy,* er likevel ikke noe som eksisterer i et vakuum, enten det er snakk om en rettighet, verdi eller tilstand. Den sosiale konteksten individer er en del av spiller inn på hvordan personvern forstås, og i en vurdering av hvilke opplysninger som anses som beskyttelsesverdige ligger automatisk en vurdering av hvilke opplysninger som *ikke* er det. Denne erkjennelsen er Helen Nissenbaums utgangspunkt for boken *Privacy in Context* (2010), der hun hevder at fokuset på personvern som et redskap for utelukkende å beskytte eller kontrollerer individets personopplysninger, er lite fruktbart. Hun hevder i stedet at «a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information» (Nissenbaum 2010, 127). Det er med andre ord umulig å vurdere hvilken informasjon som bør beskyttes og hvilken som ikke bør

det uten å ta *konteksten* informasjonsbyttet skjer i med i ligningen. Hun hevder videre at «the indignation, protest, discomfort, and resistance to technology-based information systems and practices, […] invariably can be traced to breaches of context-relative informational norms».

Basert på denne erkjennelsen har Nissenbaum utviklet et teoretisk rammeverk som hun kaller *teorien om kontekstuell integritet*. Kort fortalt hevder hun at ulike sosiale kontekster innebærer ulike informasjonsnormer (2010, 127), og når disse *kontekstavhengige normene* brytes, brytes den kontekstuelle integriteten (2010, 140). Hvor vidt en praksis kan sies å være personvernkrenkende må vurderes i relasjon til disse kontekstavhengige informasjonsnormene, som igjen må analyseres ved å vurdere aktører, informasjonstyper og overføringsprinsipper. Nissenbaum hevder at dette rammeverket ikke bare kan bidra til å vurdere allerede eksisterende praksiser som endrer flyten av personinformasjon, men også være et velfungerende verktøy for å vurdere nye.

I denne sammenheng er dette perspektivet viktig fordi det, i motsetning til mange andre perspektiver, anerkjenner viktigheten av konteksten informasjonen avgis i. Nissenbaum oppsummerer begrepet kontekster som «structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accidents, and more».

Det er grunn til å tro at internett representerer en sosial setting hvor mange fremdeles føler seg usikre og sårbare. Endringene som følger med teknologisk utvikling skjer enormt raskt. Det kan hevdes at mange fremdeles strever med å finne ut av spillereglene i denne konteksten, og at denne usikkerheten kan bidra til å forklare at personvern oppfattes som viktig, uten at det nødvendigvis gjenspeiles i handlinger.

2.6 Oppsummering

Som denne redegjørelsen har vist er personvernbegrepet, herunder også det engelske begrepet *privacy*, mangefasettert, komplekst og til tider vanskelig å gripe. Samtidig er det, hvis vi forstår personvern som en verdi, noe som de fleste av oss mener er viktig og beskyttelsesverdig. Hvordan personvern forstås har også endret seg i stor grad siden Warren og Brandeis' publiserte *The Right to Privacy* i 1890, en artikkel som regnes som startskuddet for personvernteori. Denne utviklingen må sees i sammenheng med den teknologiske utviklingen. Den økende graden av maskinelt registrerte personopplysninger i enorme

databaser førte til at Alan Westin i 1967 skilte ut *personopplysningsvern* fra tidligere forståelser av personvernet, og det er denne definisjonen som i dag dominerer personverndiskursen. I dag, nesten femti år etter Westins bok utkom, har teknologisk utvikling muliggjort et registreringsregime av en helt annen dimensjon enn man kunne forestilt seg i 1967. Dermed er det grunn til å hevde at denne forståelsen av personvern er minst like sentral i dag som for femti år siden.

På samme tid er det viktig å anerkjenne at personvern ikke er en konstant, universell verdi. Hva mennesker oppfatter og vurderer som privat og beskyttelsesverdig varierer enormt både mellom kulturer og subkulturer, historiske epoker og til og med fra individ til individ (Nissenbaum 2010, 107), avhengige av den sosiale konteksten. Følgelig vil denne konteksten som personopplysninger avgis i spille en nøkkelrolle i hvordan vi vurderer hvor vidt personvernet krenkes. Kulturelle forskjeller manifesterer seg ofte gjennom hvilken vekt man tillegger personvern i møte med konkurrerende interesser (Solove 2004, 183). Det kan videre tenkes at internett representerer en kontekst hvor spillereglene fullt ut ikke forstås av alle, i tillegg til at de stadige endringene og teknologiske nyvinningene gjør det til et uoversiktlig og komplisert felt å fullt ut forstå. Dette er tema for neste kapittel.

3 Personopplysninger til salgs

Personopplysningsvern har som nevnt de siste snaue femti årene fått et stadig sterkere fotfeste som den sentrale hovedkategorien innen personvernproblematikk. Denne måten å forstå personvernbegrepet på skriver seg som nevnt fra Alan Westins bok *Privacy and Freedom* (1967). Siden Westin tok til orde for et sterkt vern av personopplysninger i digitale databaser i 1967 har imidlertid den teknologiske utviklingen skutt enorm fart, og tempoet synes ikke å avta. Måten vi har inkorporert og gjort oss avhengige av stadig ny teknologi i hverdagen de siste 45 årene er fundamental og altomfattende, og stadig mer avanserte elektroniske verktøy benyttes av stadig flere, både statlige og kommersielle institusjoner, så vel som privatpersoner.

Hva er annerledes i dag?

Personinformasjon som registreres og lagres digitalt ved hjelp av moderne datateknologi inntar en del egenskaper, og disse egenskapene påvirker forutsetningene for et godt personopplysningsvern. Karen Spärck Jones (2003) oppsummerer disse egenskapene som *varighet, volum, usynlighet, nøytralitet, tilgjengelighet, reorganisering* og *avstand*. Flere av disse egenskapene, som varighet, volum, usynlighet og tilgjengelighet er selvforklarende. Det er likevel verdt å kort diskutere de ulike hver for seg.

At informasjonen er varig og voluminøs muliggjør eksistensen av enorme databaser med personinformasjon. Disse databasene har skapt begrepet *data mining*, altså datagruvedrift, en industri med negative konsekvenser for personvern på internett (Hamelink 2000, 133). Metaforen antyder altså at databasene er gruver, hvor kompetente gruvearbeidere kan finne gull, altså grave frem verdier fra tilsynelatende verdiløs jord. En bieffekt av at det er blitt mye billigere å lagre store mengder data er at det for selskapene som sitter på opplysningene aldri vil lønne seg å slette dem (Mayer-Schönberger og Cukier 2013, 100 – 101). Å beholde opplysningene vil alltid være det mest lønnsomme, siden den potensielle verdien som ligger i sammenstilling av store datamengder er stor, og kostandene for lagring er lav. Dette skiftet har medført fremveksten av «et omfattende og lukrativt marked for personlig informasjon om praktisk talt alle» (Shapiro 1999, 158). Dette markedet vil være hovedfokus i denne delen av oppgaven. Hovedpoenget i denne sammenheng er at dette markedet har vokst, og fortsetter å vokse, som en direkte konsekvens av endringer vedrørende dataenes volum, samt varigheten.

Usynlighet innebærer at personinformasjon er tilgjengelig for mennesker som er usynlige for datasubjektet. Med *nøytralitet* menes at dataene er løsrevet fra sin opprinnelige kontekst, og dermed kan feiltolkes. *Tilgjengelighet* peker på hvor enkelt personinformasjon kan letes frem av andre. Den relaterte egenskapen *reorganisering* innebærer at informasjon kan settes sammen på nytt, uavhengig av den originale konteksten. Endelig peker egenskapen *avstand* på at den digitale informasjonen kan eksistere i fysiske rom langt vekke fra personen informasjonen gjelder. Facebooks enorme servere i USA inneholder for eksempel enorme mengder informasjon om dets mange hundre millioner brukere, fjernt fra opprinnelseslandene.

Disse egenskapene ved den teknologiske utviklingen påvirker personvernet hver for seg, men kombinasjonen av at alle virker sammen er enda større (Spärck Jones 2003, 290). Joinson og Paine (2007, 246) fremhever i sin gjennomgang av Spärck Jones at internettets iboende egenskap *tilkobling* bidrar til å forverre de allerede personverntruende egenskapene ved moderne elektronisk teknologi.

I tillegg har det de seneste årene skjedd en markant endring i hvilke typer personinformasjon som registreres. På Westins tid, da forståelsen om personvern som relatert til maskinell registrering av personopplysninger vant fram, var snakk om skrift og tegn mediert ved hjelp av datamaskiner. Schartum og Bygrave (2011, 26) observerer to iøynefallende utviklingstrekk siden den gang. For det første har informasjonsbehandlingen kommet til å innebefatte flere ting enn skrift og tegn, som for eksempel bilde og video, noe som har ført til at personopplysninger har flere uttrykk enn tidligere. For det andre registreres personopplysninger på flere måter enn tidligere, ved hjelp av stadig kraftigere sensorer som finnes i alt fra smarttelefonene vi bærer med oss til overvåkningskameraer som ser ned på oss. Dermed blir «stadig større deler av vår fysiske verden registrert ved hjelp av teknologi som automatisk genererer opplysninger om oss» (Schartum og Bygrave 2011, 26).

3.1 Personopplysninger som handelsvare

Dagens internett baserer seg som nevnt i stor grad på en modell som innebærer at innhold og tjenester tilbys gratis i bytte mot personinformasjon (Shapiro 1999, 160, Andrejevic 2014, 92-97, Papacharissi 2010a). I mange tilfeller skjer dette «informasjonsbyttet» i tillegg uten at nettbrukeren er klar over det (Hamelink 2000, 133, Shapiro 1999, 159). Nettsurfing, bruk av

søkemotorer og elektronisk betaling innebærer som regel at man etterlater seg et digitalt fotspor, som potensielt kan si mye om ditt digitale liv, og dermed om deg. Kroppsnær teknologi innebygget i de stadig mer avanserte smarttelefonene vi bærer med oss genererer lokasjonsinformasjon ved hjelp av stadig bedre GPS-målere. Apper installert i smarttelefonene vi bærer med oss kan måle puls, kroppstemperatur, søvnmønster og den generelle helsetilstanden din gjennom stadig kraftigere sensorer. Papacharissi og Fernback (2005, 260) skriver at «through the increasing sophistication of data mining tools, consumer data base creation and management has become a growing, profitable enterprise», og hevder at en følge av dette er at den digitale markedsøkonomien og personvern er to elementer på kant med hverandre.

Eiendomsrettsperspektivet

Schartum og Bygrave (2011, 47) er på den annen side i utgangspunktet kritiske til en *eiendomsrettstilnærming* til personvernspørsmål, fordi personvern primært omhandler «ivaretakelse av ideelle verdier og interesser, der økonomiske spørsmål er blant de forhold som personvernet skal veies opp imot». De avskriver imidlertid ikke et slikt eiendomsperspektiv fullstendig, av to grunner. For det første påpeker de at et slikt perspektiv bygger på to grunnleggende verdier i vårt samfunn, nemlig menneskets selvbestemmelsesrett og verdighet. For det andre påpeker de at et slikt syn passer inn i det moderne informasjonssamfunnet, da personinformasjon ofte har økonomisk verdi, og disposisjonsretten over opplysningene dermed henger sammen med retten til å disponere de økonomiske verdiene.

Andrew L. Shapiro (1999, 163), som i likhet med Schartum og Bygrave har juridisk bakgrunn, beskriver den samme kritikken som en overgripende *commodification critique*, et begrep hentet fra marxistisk tenkning, som kort fortalt omtaler hvordan kapitalismen transformerer stadig flere deler av vår verden til salgbare enheter på et marked. Å redusere personvern til en vare på et marked sammenlignes ifølge en slik kritikk med å etablere et marked for ytrings- eller religionsfrihet. Shapiro (1999, 163) nyanserer dette bildet noe ved å påpeke at amerikansk lovgivning beskytter det tradisjonelle personvernet i større grad enn det moderne personopplysningsvernet, og fremhever dette som en viktig forskjell mellom amerikansk og europeisk personvernlovgivning.

Det er interessant at teoretikerne med bakgrunn fra andre fagfelt enn det juridiske tilsynelatende uten tvil slår fast at personopplysninger *er* en salgbar vare på et marked, mens juristene Shapiro, Schartum og Bygrave åpner opp for et mer nyansert syn. Dette kan sannsynligvis forklares med at en strengt juridisk tilnærming til personvernproblematikk har et snevrere fokus enn bredere anlagt samfunnsvitenskapelige tilnærminger. I tillegg kan man hevde at Shapiro og Schartum og Bygraves nyansering er av konseptuell art, og har et normativt utgangspunkt, altså at perspektivet bidrar med overgripende, normative innsikter i større grad enn observasjoner av faktiske realiteter.

Jeg vil hevde at det, til tross for denne utvilsomt viktige nyanseringen, kan slås fast at personopplysninger kjøpes og selges på et marked, og at dette markedet genererer store verdier for selskapene involvert i handelen. Papacharissi (2010b, 42 – 43) slår for eksempel ettertrykkelig fast at koblingen mellom fremveksten av avansert datateknologi og kapitalisme i moderne demokratier har ført med seg en sfære hvor personlige handlinger transformeres til salgbare enheter på et marked, med et dystert syn på konsekvensene for personvern i informasjonssamfunnet:

> Privacy, as we have known it, becomes a property of the past, as it ceases to be a good collectively defined, but is rather a property personally delineated, negotiated, or surrendered (Papacharissi 2010b, 47).

En linje kan trekkes fra Shapiro og Schartum og Bygraves kritikk av eiendomsrettstilnærmingen til Papacharissis tilstandsrapport, i det at hun beskriver personvern som noe som *var* en kollektivt definert rettighet, til noe som *er* en enhet som privatpersoner selv avgrenser, forhandler med og oppgir. I tillegg til det nevnte synet på personvern som en vare på et marked er det verdt å merke seg overgangen fra det kollektive til det individuelle i sitatet. Eiendomsrett er som kjent en individuell rettighet.

Problemer

Dette markedet har flere problemer, som på ulike måter utfordrer personvernet. Jeg vil kort redegjøre for noen av disse utfordringene, før jeg diskuterer hver enkelt mer detaljert. Det er innledningsvis viktig å understreke at det ikke er snakk om strengt atskilte kategorier, men snarere problemer som spiller sammen og overlapper hverandre.

Markedet for kjøp og salg av personopplysninger er for det første preget av et veldig *skjevt maktforhold* mellom kjøper og selger (Hamelink 200, 133, Shapiro 1999, 162, Solove 2004, 82). Som selger står enkeltindividet alene i møte med store, teknologisk og juridisk kompetente selskap.

Denne skjevheten forverres ytterligere av *kunnskapsgapet* som eksisterer. Flere undersøkelser har vist at det er stor avstand mellom hva brukere av internettjenester tror de vet og selskapenes faktiske praksis (Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007).

Dette kunnskapsgapet kan hevdes å henge sammen med problematiske sider ved *kontraktene* brukere undertegner for å få tilgang på tjenester, ofte representert som *personvernerklæringer*. Disse er ofte vage, preget av vanskelig språk og fungerer mer som et juridisk sikkerhetsnett for selskapene enn en brukervennlig rettledning (Schwartz 2000, 823, Sovern 1999, 1099, Solove 2004, 82, Pollach 2007, 104, Papacharissi og Fernback 2005, 265).

I tillegg til disse problemene relatert til den konkrete avtaleinngåelsen kan man hevde at en rettferdig byttehandel uansett er en illusjon, fordi det er umulig å vurdere verdien av opplysningene som selges (Solove 2004, 87 – 88, Froomkin 2000, 1502 – 1503). Denne *umulige verdivurderingen* kommer av at hver informasjonsenhet alene ikke er særlig verdifull, men har potensiale til å bli det, sammenstilt med annen informasjon. Denne aggregeringseffekten medfører at heller ikke selskapene med sikkerhet kan fastslå en informasjonsenhets verdi. Det de derimot kan fastslå er at sannsynligheten for en stor verdiøkning er stor, og kostnadene for lagring er lav, og at det dermed alltid vil lønne seg å beholde informasjonen.

At byttehandelen skal kunne kalles rettferdig forutsetter også at det eksisterer *et reelt alternativ* til å inngå avtalen. Det er sjeldent tilfelle. Å velge bort internettjenester som epost, sosiale medier og netthandel, å avslutte sitt digitale liv, vil føre med seg store kostnader (Lüders 2008, 104 – 105). Både det sosiale og profesjonelle livet forutsetter en grad av tilstedeværelse på nett.

I tillegg til disse problemene, som relaterer til individet i møte med selskaper gjennom de konkrete avtaleinngåelsene, er det verdt å peke på en potensiell fare på et kollektivt nivå, utviklingen av et *digitalt personvernskille* (Papacharissi 2010a, Papacharissi 2010b, 46 – 47).

Undersøkelser har i tillegg demonstrert hvordan personvernerklæringer ofte er skrevet på et språk som overgår de antatte leseferdighetene til en stor del av kundemassen (Antón et al. 2003, 2, Jensen og Potts 2004, 477, Pollach 2007, 104). Digitale ferdigheter er i tillegg i utgangspunktet ujevnt fordelt i befolkningen, både innad i land og internasjonalt, og disse ujevnhetene speiler eksisterende sosiodemografiske ulikheter for øvrig (Hargittai 2008, 937). I tillegg er det en logisk konsekvens av en kommersialisering av personvernet at noen ikke vil ha råd til å kjøpe seg fri.

3.2 Skjevt maktforhold – hvem har ansvaret?

Det første problemet med markedet for personopplysninger er at maktforholdet mellom kjøper og selger sjeldent vil være likeverdig (Solove 2004, 82, Hamelink 200, 133, Shapiro 1999, 162). Å forhandle fram andre vilkår enn de som selskapet man forhandler med har stipulert vil kreve kunnskap og kapasitet de færreste besitter. Siden disse selskapene i tillegg tjener store summer på personopplysningene vil den juridiske motstanden de forsvarer praksisen med sannsynligvis være formidabel. I tillegg gjør den enorme kundemassen at en enkeltbrukers protest og eventuelle boikott av tjenestene vil være ubetydelig i det store bildet.

Man kan imidlertid argumentere for at det skjeve maktforholdet til en viss grad kan rettes opp gjennom å styrke markedet for *personopplysningsvern*, i kontrast til og i konkurranse med markedet for *personopplysninger* (Shapiro 1999, 159). En slik utvikling vil imidlertid innebære en forflytting av ansvar, fra myndigheter til individer, et ansvar det ifølge Shapiro er naivt å tro enkeltpersoner har kapasitet til å ta. En slik tro på enkeltindividet som sin egen «personvernmegler» forutsetter en tro på at enkeltindividet kan utføre et oppdrag «så komplekst at det til dags dato forvirrer de fleste regjeringer» (Shapiro 1999, 161).

En forflytting av ansvaret for trygg ivaretakelse av personopplysningsvern, fra myndigheter til individ, legger med andre ord uforholdsmessig mye ansvar på enkeltindividet. I tillegg er det ifølge Paul M. Schwartz (1997, 50) lite sannsynlig at individer har redskapene til å uttrykke personvernpreferanser på et kollektivt nivå: «A critical mass of sophisticated privacy consumers is not yet emerging» (Schwartz 2000, 822).

Det er også grunn til å være varsom med å forvente at virksomhetene er skikket til å forvalte ansvaret for personvern på nett, siden disse selskapene gjerne har liten interesse av å avgi optimal informasjon (Schwartz 1999, 1684). Samme forfatter skriver at «data collectors have

an incentive to engage in smokescreen tactics to make it difficult for individuals to obtain understandable information about data collection and use» (Schwartz 2004, 2080). Dette er imidlertid i stor grad det talspersonene for et marked for personopplysninger fremholder som den optimale løsningen, spesielt forkjemperne for minst mulig statlig regulering.

3.3 Kunnskapsgapet

Én av grunnene til at maktforholdet mellom kjøper og selger ikke kan sies å være likeverdig er kunnskapsgapet som eksisterer mellom hva brukerne *tror* skjer med personinformasjonen de avgir på internett og faktisk praksis. Andrejevic (2009, 50) skriver at «[p]ublic awareness of the extent and character of, for example, online monitoring, lags behind industry practice». Flere undersøkelser har påvist et enormt gap mellom nettbrukeres forståelse av personvernregler og faktisk praksis hos nettselskapene (Turow 2003, Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007). Nettbrukere vet rett og slett ikke implikasjonene av å benytte internettjenester. Turow (2003, 19) skriver at «adults with internet connections at home are ignorant, even naïve, about the way data about them flows behind their screens».

Hoofnagle and King (2008, 26) observerer på lignende vis at en majoritet av respondentene i undersøkelsen trodde at tilstedeværelsen av en personvernerklæring (privacy policy) sikret brukeren fra videresalg av personopplysninger til en tredjepart. Slike personvernerklæringer sikrer imidlertid ikke brukeren bestemte rettigheter, men er mer å regne som en erklæring av selskapets *privacy policy*, og stipulerer ofte nettopp den praksisen forbrukeren tror en slik personvernerklæring forbyr. Forbrukere tolker altså ofte slike personvernerklæringer som et «godkjentstempel» som garanterer etterlevelse av en rekke prinsipper (Hoofnagle and King 2008, 2), noe som sjeldent er en riktig forståelse av slike erklæringer. I virkeligheten er personvernerklæringene nemlig et godkjentstempel på at brukeren tillater utstrakt bruk av personopplysningene som registreres, altså det stikk motsatte av hva brukerne ofte tror.

En fersk undersøkelse gjennomført av PEW slår fast at hele 52 % feilaktig tror en personvernerklæring er synonymt med konfidensialitet (Smith 2014, 7). Dette spørsmålet er trukket direkte fra en tidligere undersøkelse fra Annenberg Public Policy Center , hvor 57 % svarte feilaktig på samme spørsmål (Turow 2003, 19). Det er altså grunn til å hevde at amerikanske nettbrukere kun har gjennomgått en marginal bevisstgjøring vedrørende dette

temaet de siste ti årene. I forbindelse med sistnevnte undersøkelse skriver Turow (2003, 19) at «[d]espite strong concerns about government and corporate intrusions, American adults who use the internet at home don't understand the flow of their data online».

Schwartz (1999, 1683 – 1684) peker også på kunnskapsgapet som en faktor som hindrer et marked for personopplysninger i å fungere. Samme forfatter fremsetter to forklaringer på hvordan dette kunnskapsgapet oppstår: For det første peker han på nettets for de fleste ugjennomsiktige, tekniske infrastruktur. For det andre er internettselskapene, med overlegen kunnskap om den samme tekniske infrastrukturen, ikke tjent med å avgi optimal informasjon til kundene, all den tid denne informasjonen tjener som basis for forretningsvirksomheten (Schwartz 1999, 1684 – 1685). Man kan altså hevde at brukernes kunnskapsmangel er en forutsetning for det skjeve maktforholdet diskutert i avsnittet over. Én part sitter med teknisk og juridisk spisskompetanse, i tillegg til enorme økonomiske muskler, og det eksisterer åpenbare insentiver for den samme parten til ikke å avgi optimal informasjon. Det er dermed lite sannsynlig at den andre parten, forbrukeren, skal overkomme dette gapet på egen hånd.

3.4 Problemet med en kontrakt

Et annet problem med et marked der enkeltindivider selger personinformasjon i bytte mot tjenester er kontrakten som stipulerer vilkårene brukeren må godta for å få tilgang til tjenesten. Prinsippet om informert samtykke er ifølge Kerr et al. (2009, 12) knutepunktet – *the nexus* – for interaksjonen mellom mennesker og de stadig mer automatiserte metodene for informasjonsinnsamling som vi interagerer med. Dagens Personopplysningslov baserer seg på at individet skal kunne gjøre frie valg basert på individuelle interesseavveiinger, gjennom avgivelse av samtykke (Schartum og Bygrave 2011, 44), og dette samtykket avgis på internett som oftest i form av en personvernerklæring.

Forbrukeren er i møte med disse kontraktene prisgitt vilkårene selskapene fremsetter, og har ingen reell forhandlingsmakt, noe som resulterer i at individet ofte godtar vilkårene de får servert uten reelle forhandlinger (Schwartz 2000, 823). Disse vilkårene er i tillegg ifølge Jeff Sovern (1999, 1099) preget av «tørt, juridisk og uinteressant språk». Flere undersøkelser har vist at mange ikke engang leser dem (Andrejevic 2014, 99), og at de er dårlige egnet som redskaper for informerte avgjørelser på grunn av blant annet tilgjengelighet og lesbarhet (Jensen og Potts 2004, 477, Pollach 2007, 104).

Både Solove (2004, 82), Pollach (2007, 104) og Papacharissi og Fernback (2005, 265) hevder at dette kan forklares med at disse vilkårene ikke representerer en meningsfylt kontrakt, men heller bør forstås som en kunngjøring av selskapets personvernsretningslinjer. Måten disse er utformet på gir ingen garantier, men er i stedet preget av vage hentydninger om personvern og sikkerhet. De sier som regel ingenting om etablerte juridiske prinsipper om informasjonsbehandling, som for eksempel hva opplysningene kan brukes til, hvem som har tilgang til opplysningene eller hvilke muligheter som eksisterer for å få tilgang til informasjonen ved et senere tidspunkt (Solove 2004, 83).

Til tross for dette har undersøkelser vist at tilstedeværelsen av en personvernerklæring fungerer som et tillittsstempel for brukerne (Jensen, Potts og Jensen 2005, 223), uavhengig om disse leses eller ikke. Tall fra Personvernundersøkelsen (2013) demonstrerte på lignende vis at tilstedeværelsen av en personvernerklæring «teller positivt» for 81 prosent av respondentene (Datatilsynet 2013). Det er med andre ord grunn til å hevde at personvernerklæringer ofte fungerer som et tillitsstempel, til tross for at forbrukerne ikke bare tillegger disse overdrevent stor betydning, men også ofte fundamental misforstår hva de egentlig godtar.

En gjennomgang av personvernerklæringer på internett, gjennomført av The Global Privacy Enforcement Network (GPEN) i 2013, bekrefter i stor grad dette synet. En sjekk av personvernerklæringene på 2,276 nettsider og mobilapplikasjoner avslørte blant annet at 23 prosent ikke hadde en personvernerklæring overhode, en tredjedel ikke formidlet relevant informasjon og en tredjedel var skrevet på et lite leservennlig språk (Global Privacy Enfocement Network 2013). McDonald og Cranor (2008, 563) beregnet i en annen undersøkelse tiden det ville tatt for en gjennomsnittsamerikaner å lese alle personvernerklæringene han eller hun blir eksponert for ord for ord til 40 minutter per dag, eller litt over halvparten av den totale tiden brukt på internett (72 minutter). Det synes åpenbart at dette funnet innebærer at de aller færreste faktisk leser disse.

Selve språket i personvernerklæringer har også vist seg å fungere dårlig som verktøy for personvernbevisste internettbrukere. Pollach (2007, 107) konkluderer sin lingvistiske analyse av personvernerklæringer på internett med følgende dom: «online privacy policies have been drafted with the threat of privacy litigations in mind rather than commitment to fair data handling practices». Denne konklusjonen er nær identisk med Papacharissi og Fernbacks (2005, 265) funn i en lignende undersøkelse.

Lawrence Lessig beskriver praksisen med informert samtykke gjennom en skriftlig personvernerklæring på nett som et tilfelle av at myndigheter har forsøkt å løse en utfordring ved hjelp av juridiske verktøy fra en pre-internett tidsalder:

> Cluttering the web with incomprehensible words will not empower consumers to make useful choices as they surf the web. If anything, it drives consumers away from even attempting to understand what rights they give away as they move from site to site (Lessig 2006, 226 – 228).

Det er med andre ord grunn til å hevde at kontraktene vi inngår med selskapene, der personinformasjon byttes mot tilgang på tjenester, ikke fungerer på en slik måte i praksis som de er ment å gjøre formelt og juridisk for brukerne. For selskapene derimot fungerer de som trygge, juridiske forsikringer for utstrakt bruk og økonomisk inntjening i den voksende *data mining* industrien. Ironien er dermed tung når disse kontraktene ofte bærer navnet *personvernerklæring.*

3.5 Å vurdere verdien av personopplysninger

Et relatert problem i markedet for personopplysninger har med verdivurdering å gjøre. Å forstå personinformasjon som en vare som kan kjøpes og selges på et marked forutsetter at varens verdi kan vurderes, og skal byttehandelen være rettferdig må begge parter vurdere verdien av salgsobjektet noen lunde likt. Det er flere grunner til at verken individer eller selskaper kan forventes å gjøre en slik vurdering. For det første er hver lille bit av informasjon i seg selv ikke veldig verdifull på tidspunktet byttehandelen finner sted. Det er *aggregeringseffekten* av enorme mengder informasjon som til sammen blir verdifull, og dermed kan verdien av hver enkelt informasjonsenhet umulig vurderes når man avgir bare en del av det store bildet av gangen (Solove 2004, 87 – 88). Ifølge A. Michael Froomkin (2000, 1502 – 1503) vil ikke engang mennesker med høy bevissthet rundt personvern ha mulighet til å sette en riktig pris på informasjonen de avgir, rett og slett fordi verdien av hver informasjonsdel øker i takt med den samlede mengden informasjon som samles inn. Han kaller dette fenomenet *privacy myopia*, eller personvernnærsynthet.

Verdien av informasjonsenhetene som inngår i byttehandelen er altså umulig å fastsette på tidspunktet den samles inn. Som en følge av stadig billigere og bedre lagringsmuligheter er det likevel aldri lønnsomt for selskapene å kvitte seg med data når de først er samlet inn, nettopp fordi fremtidig sammenstilling og analyse kan trekke verdier ut av disse, i tillegg til at

lagringskostnadene er så lave (Mayer-Schönberger og Cukier 2013, 100 - 101). I mange tilfeller er det den potensielle verdien på et tidspunkt langt frem i tid som motiverer den storstilte datainnsamlingen og lagringen. Det er derfor grunn til å hevde at heller ikke selskapene som registrerer informasjonen kan gjennomføre en korrekt verdivurdering når informasjonen samles inn, simpelthen fordi verdien kan, og vil, øke enormt en gang i fremtiden. Det oppstår dermed en situasjon de færreste økonomer ville vurdert som en rettferdig byttehandel: ingen av partene kan med sikkerhet fastslå verdien av enheten det forhandles om, men kun én part vil ha mulighet til å profittere på den når den en gang i fremtiden genererer verdi.

3.6 Fravær av alternativer til registreringsregimet

Å underkaste seg registreringsregimet som dagens internettmodell krever, er et valg mennesker i informasjonssamfunnet tar hver eneste dag. Dette valget er imidlertid ikke nødvendigvis å forstå som helt fritt. Schartum og Bygrave (2011, 49) skriver at «kravet om «etablert tillitsforhold» uttrykker behovet for at behandling av personopplysninger i størst mulig grad skal hvile på et tillitsforhold mellom den registrerte og den behandlingsansvarlige». Datatilsynets undersøkelse viste at sosiale nettsamfunn og nettbutikker har svært liten tillitt i den norske befolkningen. 80 % har ingen eller liten tillit til sosiale nettsteder, mens tilsvarende tall for nettbutikker er 61 % (Datatilsynet 2013). Slike virksomheter selger på samme tid personopplysninger videre i større grad enn for eksempel offentlige etater. Videre kobler Schartum og Bygrave (2011, 50) kravet om etablert tillitsforhold med «bestemmelser om at det i visse tilfeller må innhentes et frivillig og informert samtykke for at behandlingen av personopplysninger skal være lovlig». Et slikt samtykke må være «frivillig», «uttrykkelig» og «informert» (Schartum and Bygrave 2011, 161).

Hovedpoenget med denne redegjørelsen er at «frivillig» innebærer at det ikke er knyttet negative konsekvenser til å ikke gi sitt samtykke. Hva «negative konsekvenser» innebærer er åpenbart et tolkningsspørsmål, men det er grunn til å hevde at de negative konsekvensene knyttet til å ikke underkaste seg registreringsregimet dagens internettmodell forutsetter er betydelige. Å velge å ikke godta vilkårene for registrering innebærer nemlig å avstå fra tilgang til tjenester som har blitt en integrert del av dagliglivet, og vil innebære et stort tap: Andrejevic (2009, 52) skriver at «[c]onsumers are entering a world in which access to the

goods and services they seek *requires* willing submission to increasingly detailed forms of data collection and online monitoring».

Papacharissi (2010b, 47) fremhever på samme måte at å velge å *ikke* selge sine personopplysninger innebærer en sosial ulempe. Personvern blir en vare som byttes mot tilgang til tjenester som er en selvfølgelig del av hverdagen i et informasjonssamfunn. Marika Lüders (2008, 104 - 105) beskriver denne valgmuligheten som et «dilemma med to ufordelaktige alternativer»: Man kan enten beskytte eget privatliv ved en fullstendig tilbaketrekning fra internett eller sette personvernet i fare.

3.7 Et digitalt personvernskille

Problemene jeg har drøftet så langt dreier seg om problemer i enkeltindividets møte med internettselskapene. Det siste punktet jeg vil ta for meg er av mer kollektiv art. Et rendyrket marked for kjøp og salg av personopplysningsvern vil nemlig også være ufordelaktig for de som ikke har råd til å kjøpe seg en slik vare.

Papacharissi (2010a, 2010b, 46 – 47) hevder at en følge av at personlig informasjon transformeres til valuta på et marked er at personvern erverver en luksusvares karakteristikker. Hun oppgir to grunner til dette. For det første vil det bli for dyrt for gjennomsnittsindividet å oppnå og holde fast ved eget personvern. For det andre vil det innebære en sosial ulempe å ikke forsake en del av eget personvern, når det man bytter til seg er tjenester og varer assosiert med hverdagslivet i informasjonssamfunnet (Papacharissi 2010b, 47). Dette er i tråd med Marika Lüders (2008, 104 - 105) syn på byttehandelen med personopplysninger som et «dilemma med to ufordelaktige alternativer». I tillegg peker Papacharissi (2010a) på at tilgang til denne luksusvaren krever et nivå av internettferdighet de fleste ikke innehar. Det logiske resultatet blir et personvernskille, som i tillegg vil speile dominerende sosiodemografiske ulikheter (Hargittai 2008, 937).

Flere undersøkelser har på lignende vis vist at personvernerklæringer på internett er skrevet på et språk som krever leseferdigheter over det antatte gjennomsnittet av internettbrukere i USA (Antón et al. 2003, 2, Jensen og Potts 2004, 477, Pollach 2007, 104). Man kan dermed hevde at i sin nåværende form bidrar personvernerklæringer til å skape et personvernskille basert på leseferdigheter, som igjen har nær sammenheng med eksisterende sosiodemografiske ulikheter (Hargittai 2008, 937).

3.8 Oppsummering – et forestilt personvernparadoks?

Alle disse aspektene ved den kommersielle modellen dagens internett baserer seg på kan i sum oppsummeres med at individet – produsenten av det digitale gullet – stiller svakt i møte med internettselskapene. Alle disse problemene ved den kommersielle modellen internett i så stor grad baserer seg på har følger for forståelsen av det som er blitt kalt *personvernparadokset* (Barnes 2006, Norberg, Horne og Horne 2007, 101). Flere undersøkelser har vist at bekymringen for personvernets kår er stor uten at disse holdningene fører til store protester eller boikotter av denne praksisen. Personvernbevisste individer opptrer ikke som personvernbevisste forbrukere på internett. Alle disse problemene ved markedet for personopplysninger har som logisk konsekvens at én av forutsetningene for å forstå dette som et paradoks faller bort. Hvis man ikke *vet* hva et samtykke innebærer, hvis man ikke *forstår* hva et samtykke innebærer og til sist, hvis det ikke eksisterer *alternativer* til å akseptere praksisen – kan det da virkelig kalles et paradoks?

Å forvente at individer skal ha kompetanse og kapasitet til å beskytte sitt eget personvern i et privat personvernmarked uten hjelp fra myndigheter er i tillegg, ifølge Andrew L. Shapiro (1999, 161) farlig naivt. Like fullt er denne byttehandelen uunngåelig for å nyte godt av alle bekvemmelighetene som eksisterer, og som vi i stor grad er avhengige av i dagliglivet.

Mark Andrejevic tolker denne byttehandelen som en form for overvåking. Den kommersielle strukturen store deler av internett er basert på forutsetter ifølge ham at individet forplikter seg til underkaste seg overvåking i bytte mot digitale varer og tjenester (Andrejevic 2014, 97). Den formelle avtaleinngåelsen skjer idet brukeren godtar en personvernavtale for bruk av tjenesten. Å forstå denne avtaleinngåelsen som en aksept for vilkårene er ifølge Andrejevic problematisk fordi det er stor forskjell mellom den type samtykke et klikke på «godta» - knappen innebærer og *informert* samtykke, noe Andrejevic' (2014: 99) undersøkelse viste, og som dette kapittelet har diskutert utfyllende. Personvernvilkår kan også endres etter tidspunktet for avtaleinngåelsen, noe Facebook skapte en del oppstyr med i 2010 (Hargittai og boyd 2010).

Obligatorisk frivillighet

Gary T. Marx (2006, 2) kaller denne metoden *obligatorisk frivillighet*, en form for *myk overvåkning.* Denne typen overvåkning skiller seg fra de «harde» formene, i kraft av at de overvåkede tilsynelatende avgir personopplysningene frivillig, eller frivillig samtykker til personverninngripende tiltak. Det er imidlertid – igjen – grunn til å stille spørsmålstegn ved hvorvidt denne frivilligheten virkelig innebærer et reelt valg, et poeng Marx eksemplifiserer med følgende kunngjøring fra en kanadisk flyplass: «Notice: Security measures are being taken to observe and inspect persons. No passengers are obliged to submit to a search of persons or goods if they choose not to board our aircraft» (Marx 2006, 2). Det informeres altså om at ingen behøver å godta en mulig ransakelse av person eller bagasje, *så lenge man ikke boarder flyet.* Det gis altså et valg, men for de aller fleste vil det ikke være et reelt alternativ å ikke gjennomføre reisen. I det minste er det et alternativ med store negative konsekvenser for enkeltindividet.

Dette perspektivet ligger tett opp mot Marika Lüders syn på byttehandelen med personinformasjon som «et dilemma med to ufordelaktige alternativer» (2008, 104 – 105). Hennes utgangspunkt er sosiale nettverkstjenester, men observasjonene har gyldighet for alle tjenestetilbydere som benytter samme modell. Lüders' dilemma er følgelig

> Enten å beskytte eget privatliv ved å unngå sosiale nettverkstjenester, på tross av potensielt uønskede personlige og sosiale konsekvenser. Eller å velge å være til stede på nettet og dermed sette eget personvern i fare (Lüders 2008, 104 – 105).

Ian Kerr et al. (2009, 7) setter Marx' tanker om myk overvåkning i en større sammenheng, og hevder at det er en del av et skifte mot en økende bruk av myk paternalisme. De beskriver dette som en erkjennelse fra myndigheter side av at det er mer effektivt å «veilede» innbyggerne til å foreta fornuftige valg enn å forby ufordelaktige valgmuligheter – hard paternalisme. Ifølge forfatterne har mange myndigheter og selskaper som er involvert i informasjonshandel innsett at en mykere form for informasjonsinnsamling fungerer vel så godt som gammeldags overvåkning. Disse perspektivene kobler altså den tilsynelatende mer uskyldige informasjonsregistreringen med hard overvåking.

Personvernproblematikkens diskusjoner kan ifølge Lüders (2008, 103) deles inn i to hovedkategorier: (1) «krenking av personlige rom fra statlige myndigheter eller kommersielle institusjoners side, blant annet ved hjelp av overvåkingsteknologi, sporing av elektroniske handlinger og bearbeiding av personlige data som finnes i elektroniske

kommunikasjonssystemer» på den ene siden og (2) «frivillig avsløring av personinformasjon til en viss grad kontrollert av individene». Denne oppgaven fokuserer i hovedsak på den andre kategorien, men jeg vil hevde at skillelinjen mellom de to kategoriene ikke nødvendigvis er hugget i stein. En av de aller viktigste innsiktene fra Snowden-avsløringene var hvor enkelt personinformasjon fløt mellom de kommersielle internettselskapene til det statlige overvåkingsorganet NSA.

4 Metode og data

I dette kapittelet vil jeg redegjøre for det metodiske opplegget for oppgaven. Jeg vil begynne med å diskutere datamaterialet som ligger til grunn for analysene, og ulike egenskaper, styrker og svakheter ved dette. Denne innledningen er nødvendig siden jeg benytter et datamateriale som er samlet inn av et profesjonelt analysebyrå, på oppdrag av Datatilsynet.

Videre vil jeg ta for meg hver enkelt av variablene jeg benytter i analysene og diskutere disse. Så følger en redegjørelse av analysemetodene som skal benyttes for å besvare de to problemstillingene hver for seg. Analyser og resultater følger i neste kapittel. Aller først vil jeg drøfte implikasjonene å bruke datamaterialet som jeg bygger oppgaven på.

Fordeler og ulemper med datamaterialet

Denne oppgaven tar nemlig utgangspunkt i data samlet inn i arbeidet med Personvernundersøkelsen 2013/2014, i regi av Datatilsynet. Analyseselskapet Opinion Perduco sto for innsamlingen av data, som foregikk i perioden 18. til 30. november 2013. Undersøkelsen ble gjennomført på web, gjennom Norstats webpanel, som er rekruttert gjennom landsrepresentative telefonundersøkelser. Populasjonen for undersøkelsen er den norske befolkningen, 15 år eller eldre, og det ble gjennomført 1 501 intervjuer, som er vektet på geografi, kjønn og alder.

Jeg fikk tilgang til datamaterialet etter å ha vært i kontakt med seniorrådgiver Catharina Nes, som på sin side kontaktet Opinion Perduco. Datatilsynet har gjennomført en rekke analyser, og disse ble publisert fortløpende i form av åtte tematiske delrapporter og én hovedrapport[2]. I tillegg ble årsrapporten *Personvern 2014 – tilstand og trender* basert på den samme undersøkelsen[3]. Alle disse er tilgjengelig på Datatilsynets nettsider, og ble gjenstand for en del medieoppmerksomhet. Oppslagene dreide seg i hovedsak om funnene relatert til Snowden-avsløringene (Tennøe og Thon 2014, Færaas 2014).

[2] Både delrapportene og hovedrapporten Personvernundersøkelsen 2013/2014 kan finnes på http://www.datatilsynet.no/verktoy-skjema/Analyser-utredninger/Personvernundersokelser/Personvernundersokelsen-2013-delrapporter/

[3] Personvern 2014 – tilstand og trender kan finnes på http://www.datatilsynet.no/verktoy-skjema/Analyser-utredninger/Personvern-2014-tilstand-og-trender/

Å ta utgangspunkt i dette materialet medfører slik jeg ser det store fordeler og enkelte, mindre ulemper. Fordelen med å støtte meg på disse tallene er at de uten tvil er mye mer omfangsrike enn noe jeg ville hatt kapasitet til å samle inn på egenhånd, både av tekniske, økonomiske og ikke minst tidsmessige årsaker. Det er grunn til å hevde at de færreste masteroppgaver baserer undersøkelsene sine på et datamateriale av slik kvalitet og omfang. Jeg vil hevde at tilgangen til dette datamateriale gir meg en unik mulighet til å undersøke tematikken på en helt annen måte enn hvis jeg skulle gjennomført datainnsamling på egen hånd. Et datasett bestående av 1501 respondenter tilhører unntakene på masternivå.

Spørreskjemaundersøkelser er en sammensatt gruppe metoder som varierer kraftig med hensyn til formål, innhold og hvordan de gjennomføres (Østbye et al 2013, 137). Det bakenforliggende motivet for datainnsamlingen påvirker med andre ord hvordan spørreundersøkelsen utformes. Datatilsynet har hovedsakelig gjennomført relativt enkle, deskriptive analyser, med fokus på frekvensfordeling, kontrollert for de demografiske variablene kjønn, alder og utdanning, i krysstabeller. Det er nærliggende å tro at Datatilsynet har fokus på å forklare funnene i en større sammenheng og holde øye på «det store bildet», og det har sannsynligvis satt sitt preg på hvordan spørreskjemaet er utformet. Det er også nærliggende å tro at viktigheten av gjennomslag i media og generell oppmerksomhet rundt den overordnede tematikken har vært viktig. Jeg kan, i motsetning til Datatilsynet, bore dypere ned i en mindre del av datamaterialet. Oppsummert mener jeg derfor at det ligger et stort potensiale i datamaterialet, som jeg vil utnytte.

Å bruke et datamateriale som allerede er analysert innebærer imidlertid at enkelte av observasjonene allerede er omtalt og publisert. Det er like fullt stor forskjell mellom å peke på en observasjon og å sette den samme observasjonen i en større, teoretisk sammenheng, slik jeg gjør i denne oppgaven. Et funn kan forstås på ulike måter alt etter som hvilke perspektiver man anlegger, og dermed er det ikke nødvendigvis en svakhet at datamaterialet ikke er uutforsket.

I tillegg vil det å støtte seg på allerede innsamlede data til en viss grad legge restriksjoner på hvilke analyser jeg kan utføre. Relatert til denne ulempen er det også verdt å nevne at en spørreundersøkelse med forskning som siktemål sannsynligvis ville vært utformet noe annerledes, med mindre variasjon i hvilke typer svaralternativer som brukes, og mer utstrakt bruk av variabler på intervall- og forholdstallsnivå. Dette innebærer for eksempel at

aldersvariabelen ville vært kodet som den faktiske oppgitte alderen, og dermed representert en forholdstallsskala, og ikke gruppert inn i alderskategorier.

Dette er imidlertid et vanlig fenomen, selv om det ikke er ideelt fra et forskningsperspektiv (Hayes 2005, 23 – 24). En spørreundersøkelse med forskning som siktemål ville for eksempel hatt mer nytte av at svaralternativene var like over hele undersøkelsen, slik at det ble enklere og sammenligne variabler. En slik utforming av spørreskjemaet ville muliggjort et bredere spekter av analyser enn hva tilfellet er slik det er utformet. Det kan også hevdes at hvis jeg hadde utarbeidet spørreskjemaet selv ville jeg hatt mulighet til å stille enda mer presise spørsmål, på bakgrunn av problemstillingen min og teori. Det er likevel en svakhet jeg mener klart oppveies av omfanget av datamaterialet jeg bruker.

Det faktum at jeg benytter meg av et allerede innsamlet datamateriale innebærer også at den metodiske prosessen og tilhørende diskusjon vil arte seg på en annen måte i min oppgave enn de fleste masteroppgaver. Selve datainnsamlingen, og metodisk refleksjon rundt denne, vil ikke oppta stor plass.

4.1 Diskusjon av variablene

På bakgrunn av problemstillingen og hypotesen er det nødvendig først å beskrive og i enkelte tilfeller problematisere og diskutere hvilke variabler jeg vil benytte i analysen. En variabels målenivå sier noe om hvor nyansert og informativt målet er (Grønmo 2004, 114). I datasettet jeg bygger oppgaven min på er de fleste variablene på ordinalnivå. Dette betyr at verdiene i variablene er gjensidig utelukkende med en rangert rekkefølge på verdiene. For eksempel er svaralternativene *helt uviktig, lite viktig, litt viktig og veldig viktig* ordnet i en bestemt rekkefølge, hvor svarene er tydelig rangerte, med en retning på rangeringen. (Grønmo 2004, 115).

De sier imidlertid i utgangspunktet ingenting om *avstanden* mellom de ulike verdiene. Å gjennomføre regresjonsanalyser, slik jeg vil gjøre, med data på ordinalnivå er fra et strengt metodisk ståsted problematisk, nettopp fordi dataene ikke nødvendigvis sier noe om *avstanden* mellom de ulike verdiene, slik som tilfellet er med data på intervallnivå (Grønmo 2004, 115). Eksempelvis sier variablene som inngår i indeksen min i utgangspunktet ikke noe om hvor vidt avstanden mellom *veldig viktig og litt viktig* er like stor som avstanden mellom

litt viktig og *lite viktig*, og dermed kan man i utgangspunktet ikke gjennomføre matematiske beregninger basert på addisjon og subtraksjon basert på disse.

Jeg velger likevel å gjennomføre analysene på denne måten fordi data på intervallnivå eller høyere er en sjeldenhet i samfunnsvitenskapen (Grønmo 2004, 115, Hayes 2005, 21). Som en konsekvens av dette er det ifølge Hayes (2005, 21 – 22) i kommunikasjonsforskning vanlig å behandle data på ordinalnivå som intervalldata, uten at dette gjør stor skade, selv om det kan være kontroversielt fra et strengt metodisk ståsted. Bruk av denne typen «kvasi-intervallvariabler» (Hayes 2005, 22) er faktisk så vanlig innen kommunikasjonsstudier at det kan finnes i lærebøker som eksempler på intervallskalaer (Hayes 2005, 21).

4.1.1 Holdningsvariabler

Den første analysen, som skal undersøke graden av sammenheng mellom ulike personvernholdninger, tar utgangspunkt i det første spørsmålet i undersøkelsen, *i hvilken grad er du opptatt av personvern.* Denne variabelen er datasettets mest generelle spørsmål, og kommer først i spørreundersøkelsen. Et slikt holdningsspørsmål i spørreundersøkelser kan være problematisk for målsetningen om å få valide og reliable svar (Østbye et al 2013, 143 – 144), fordi en persons holdning kun eksisterer i respondentens hode. Det betyr imidlertid ikke at slike mål på holdninger er uinteressante, men det er viktig å ha i bakhodet at folks holdninger om et bestemt tema, fra et metodisk ståsted, er mer flyktige og relative enn for eksempel observerte handlinger.

I den første analysen vil jeg benytte krysstabeller for å undersøke hvordan en rekke variabler fordeler seg med utgangspunkt i denne overordnede holdningsvariabelen. Ett av spørsmålene i undersøkelsen spør om villighet til å ta i bruk teknologi som på ulike måter er personvernkrenkende, henholdsvis GPS-sporing av egne barn og Google-briller[4]. Svaralternativene er (1) *bruker i dag*, (2) *kunne tenke meg å bruke*, (3) *kunne ikke tenke meg å bruke* og (4) *vet ikke*. Svaralternativ 1 og 4 er fjernet fra datasettet.

Det spørres altså om villighet til å gjennomføre handlinger, og er dermed, med mindre respondenten faktisk allerede bruker den aktuelle teknologien, et hypotetisk spørsmål. Svært

[4] Spørsmål 5: Under er en liste med tjenester/teknologier som vi ber deg svare om du som privatperson bruker i dag, kunne tenke deg å bruke eller ikke kunne tenke deg å bruke. 5.1: GPS-sporing av barna dine, 5.8: Google-briller.

få av respondentene benytter teknologien det spørres om, under 1 prosent av respondentene for hver av variablene. Når en så forsvinnende liten andel av respondentene faktisk benytter teknologien i dag, må dette spørsmålet tolkes som et holdningsspørsmål, som spør om en hypotetisk handling.

Videre vil jeg undersøke om det finnes en sammenheng mellom den overordnede holdningsvariabelen diskutert ovenfor, og konkrete, normative utsagn som eksplisitt setter personvern opp mot de konkurrerende interessene, *sikkerhet* og *bekvemmelighet*[5]. Svaralternativene i dette spørsmålet er (1) *helt uenig*, (2) *delvis uenig*, (3) *verken eller*, (4) *delvis enig*, (5*) helt enig* og (6) *vet ikke*, hvor sistnevnte er fjernet fra datasettet. Denne interesseavveiingen diskuteres utfyllende i analysekapittelet. Det er i denne omgang verdt å påpeke at det også i spørsmålet som omhandler villighet til å benytte personvernkrenkende teknologi, implisitt ligger en interesseavveiing. Forskjellen mellom interesseavveiingen i dette spørsmålet og det som setter personvern opp mot konkurrerende interesser er at det i sistnevnte spørsmål er formulert eksplisitt fra spørsmålsstillerens side, samt at disse påstandene flytter interesseavveiingen fra et *individuelt* til et *generelt* nivå.

4.1.2 Erfaringsvariabler

I den andre analysedelen vil jeg undersøke den andre problemstillingen, ved hjelp av en lineær regresjonsmodell. Siden denne tar sikte på å undersøke *om personlige negative erfaringer med tap av kontroll over personopplysninger predikerer et sterkere ønske om lovregulering*, vil jeg begynne med å undersøke variablene som beskriver dette hver for seg i bivariate, lineære regresjoner.

Spørsmål 12 og 13 spør begge om personlige negative erfaringer med personopplysninger på avveie[6][7]. Svaralternativene er (1) *ja*, (2) *nei* og (3) *vet ikke*, hvor sistnevnte er fjernet fra datasettet. Disse variablene er altså, i motsetning til holdningsvariablene jeg har diskutert ovenfor, spørsmål om konkrete erfaringer. Denne egenskapen ved variablene gjør de interessante, da det kan argumenteres for en retning i analysene. En konkret erfaring med tap

[5] Spørsmål 28: Hvor enig eller uenig er du i påstandene under? 28.7: Vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet. 28.4: Offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulige effektive tjenester.

[6] 12: Har du selv opplevd at personopplysninger om deg er kommet på avveie, eller er blitt misbrukt av andre.
[7] 13: Har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skulle deles

av kontroll over personopplysninger kan sannsynligvis føre til en holdningsendring, mens det er mer tvilsomt om en bestemt holdning til personvern påvirker hvor vidt man har opplevd tap av kontroll over personopplysninger. Det er imidlertid noen nyanseforskjeller mellom de to spørsmålene som bør diskuteres.

Det første spørsmålet fremstår som mer generelt og diffust enn det andre, som helt konkret spør om bilder. Dette er verdt å understreke fordi én av utfordringene relatert til personvern på internett er at det ofte er vanskelig å vurdere hvor mye informasjon man faktisk har gitt fra seg, blant annet på grunn av ugjennomtrengelige juridisk språk, og kunnskapsmangel, som jeg har redegjort for i teorikapittelet. I tillegg vil hvordan man svarer på det første spørsmålet avhenge av hvordan man forstår begrepet *personlig informasjon*. Det kan tenkes at mange tolker dette som å gjelde kun *sensitiv informasjon*, og dermed svarer nei på spørsmålet, til tross for at de muligens ikke har fullstendig kontroll over omfanget av registrering og lagring av personopplysninger som ikke vurderes som sensitive.

Mangelen på kunnskap kan også sannsynliggjøre at man har mistet kontrollen over personopplysninger uten selv å være klar over det. I lys av Nissenbaums syn på personvern som hensiktsmessig informasjonsflyt i stedet for kontroll og hemmelighold (2010, 2), er det grunn til å tro at typen informasjon avgjør hvor beskyttelsesverdig den vurderes som, og at dette spørsmålet dermed tolkes som et spørsmål om sensitive opplysninger, snarere enn personopplysninger som sådan.

Det andre spørsmålet som omhandler personlige negative erfaringer med tap av kontroll over personopplysninger spør i motsetning til det første spørsmålet eksplisitt om bilder. Som jeg har diskutert ovenfor er bilder høyst personlige, samtidig som digitaliserte bilder mer eller mindre har blitt standardformatet, noe som utvilsomt øker følelsen av sårbarhet. Dermed er det sannsynlig at denne konkretiseringen gjør at flere kan relatere til problemstillingen, og muligens også at flere opplever det som problematisk. I tillegg er bilder informasjonstypen som flest vet at eksisterer utenfor deres kontroll på internett (Rainie et al. 2013, 6).

4.1.3 Sosiodemografiske kontrollvariabler

Til sist vil jeg gjennomføre en sekvensiell regresjonsanalyse som i tillegg til det nevnte erfaringsvariablene vil inkludere de sosiodemografiske kontrollvariablene alder, kjønn og utdanning. Jeg mener det er hensiktsmessig å undersøke effekten disse variablene har på

holdninger til lovregulering fordi slike egenskaper ofte påvirker både atferd og holdninger. For eksempel er det grunn til å tro at lav alder øker muligheten for opplevd uønsket bildepublisering, all den tid deling i sosiale nettsamfunn er vanligst i denne gruppen. I tillegg kan det tenkes at den samme aldersgruppen har mer kunnskap om den kommersielle modellen internett i stor grad er basert på, og dermed vil være mer tilbøyelige til å ønske sterkere lovregulering. På lignende vis er det sannsynlig at høy utdanning øker kunnskapsnivået om flyten av personopplysninger på nett, og dermed fører til et sterkere ønske om lovregulering.

Samtlige variabler har blitt omkodet slik at de får et nullpunkt. Som nevnt er kategorien *alder* i datasettet dessverre omgjort til en ordinalvariabel. Denne informasjonen var i utgangspunktet på forholdstallsnivå, altså det høyeste målenivået, noe som ville muliggjort enda mer presise analyser. En slik omkoding er imidlertid ifølge Hayes (2005, 23-24) et vanlig fenomen, men like fullt begrensende for nøyaktige, kvantitative analyser. Denne omkodingen fra analyseselskapets side henger sannsynligvis sammen med Datatilsynets formål med spørreundersøkelsen, som altså har vært rapportskriving og ikke forskning, slik jeg har diskutert ovenfor. Variabelen kjønn er en naturlig dikotomi, i likhet med variablene som omhandler tap av kontroll over personopplysninger, som inngår i regresjonsanalysen. Kategorien *vet ikke* er fjernet fra samtlige variabler.

4.2 Analysemetoder

I det følgende vil jeg redegjøre for hvilke analysemetoder som ligger til grunn for analysene i neste kapittel. Samtlige analyser vil være kvantitative, siden jeg har hatt mulighet til å jobbe med et så omfattende datamateriale som jeg har. Innen forskning er det vanlig å skille mellom kvantitative og kvalitative data og analyser (Østbye et al 2013, 21). Kvantitative data refererer til data som kan tallfestes eller telles, mens kvalitative data på den annen side er erfaringsmateriale, som det ikke er hensiktsmessig å telle (Østbye et al 2013, 22). Kvantitative data vil generelt sett dekke færre egenskaper ved et stort antall enheter, mens kvalitative data vil gå mer i dybden på et mindre antall enheter (Østbye et al 2013, 22). Analysemetodene jeg har valgt vil dermed dekke få egenskaper ved et stort antall enheter. Først vil jeg redegjøre for valget av krysstabulering som analysemetode for å undersøke den første problemstillingen. Videre vil jeg forklare hensikten med å opprette en additiv indeks som avhengig variabel, før jeg til sist diskuterer de bi- og multivariate regresjonsanalysene som skal besvare den andre problemstillingen.

4.2.1 Krysstabeller

Jeg vil starte med å undersøke den første problemstillingen ved hjelp av bivariate tabellanalyser, med sikte på å undersøke sammenhengen i respondentenes personvernholdninger. Ifølge Østbye et al (2013, 178) skjer den viktigste formen for presentasjon av kvantitative analyser i form av tabeller, nærmere bestemt ved hjelp av bi- eller multivariate frekvensanalyser. Østbye et al (2013, 178) skriver videre at slike analyser, i motsetning til mer kompliserte teknikker, ivaretar den intuitive forståelsen av materialet, og lar forsker og leser holde øye med enhetene for bedre å forstå resultatene (Østbye et al 2013, 178). Tabellanalyser er også spesielt egnede for analyse av få variabler på nominal- eller ordinalnivå, med få verdier på hver variabel (Grønmo 2004, 295).

Jeg vil krysstabulere variabler som på forskjellig vis, enten direkte eller indirekte, sier noe om respondentens holdning til personvern. Denne metoden vil hjelpe meg med å undersøke sammenhengen mellom de ulike variablene som måler personvernholdninger. Jeg vil begynne med å krysstabulere det overordnede spørsmålet hvor opptatt er du av personvern med villighet til å benytte henholdsvis *GPS-sporing av egne barn* og *Google-briller*. Videre vil jeg krysstabulere den samme overordnede holdningsspørsmålet med normative utsagn som setter personvernet opp mot konkurrerende interesser, sikkerhet og bekvemmelighet.

4.2.2 Indeks som avhengig variabel

Dernest vil jeg gå videre med å undersøke den andre problemstillingen, ved hjelp av bi- og multivariate regresjonsanalyser. Siktemålet er å undersøke om *personlige negative erfaringer med personopplysninger på avveie predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett*. Som et første steg vil jeg opprette en additiv indeks, som vil fungere som den avhengige variabelen. En slik indeks skal fungere som et sammenfattende mål på en egenskap (Hjerm og Lindgren 2011, 32 – 33), og min indeksen vil bestå av indikatorer for *ønske om lovregulering av flyten av personopplysninger på nett*.

Grønmo (2004, 274) skriver at «additive indekser konstrueres ved å summere verdiene på variablene, slik at en enhets verdi på indeksen er lik summen av verdiene på indikatorene», med andre ord slår vi sammen flere variabler til én ny (Hjerm og Lindgren 2011, 33), og denne nye avhengige variabelen vil fungere som et sammenfattende mål på begrepet *ønske om lovregulering av flyten av personopplysninger på nett*.

Det finnes flere fordeler med å benytte en indeks som avhengig variabler i kvantitative analyser. For det første vil en sammenslåing av flere variabler representere en bedre operasjonalisering av et teoretisk begrep, noe som innebærer økt validitet (Hjerm og Lindgren 2011, 33). Summen av flere variabler vil med andre ord fange opp et bredere spekter av det samme begrepet enn en enkelt variabel kan. For det andre vil en indeks gjøre muligheten for tilfeldige feil mindre, og dermed gi økt reliabilitet. Hvis for eksempel én av variablene har en spørsmålsstilling som kan misforstås av respondentene, minsker dennes påvirkningskraft sammenslått med andre variabler (Hjerm og Lindgren 2011, 34).

En svakhet ved å bruke en slik indeks er at noen nyanser går tapt. At en respondent får en indeksscore på 8 kan for eksempel bety at han eller hun oppga svarene 2 – 2 – 2 – 2 på de fire spørsmålene som inngår i indeksen, altså at samtlige variabler ble vurdert som *litt viktig*. Det kan imidlertid også være at den samme respondenten oppga 0 – 2 – 3 – 3, og dermed at én kategori skiller seg ut som «helt uviktig», mens to andre vurderes som *veldig viktig.* Dette informasjonstapet er imidlertid ifølge Hjerm og Lindgren (2011, 37) som oftest ikke et problem, da formålet med å opprette indeksen er å måle en bredere dimensjon, og dermed er ikke denne eventuelle variasjonen viktig.

En indeks er ment å være et mål på et generelt begrep. Det er derfor viktig at avgjørelsen om hva som skal inngå i indeksen er teoretisk og begrepsmessig fundert (Skog 2010, 96, Hjerm og Lindgren 2011, 34). Min indeks vil ta utgangspunkt i spørsmål 3. *Er det noen opplysninger om deg eller andre som du mener lovverket særlig bør beskytte mot innsamling og videre bruk?* Spørsmålet omhandler altså lovregulering av innsamling og videre bruk av opplysninger. Fra de 14 svaralternativene har jeg valgt ut de fire som jeg vil argumentere for omhandler flyten av personopplysninger på nett: (8) *Opplysninger om steder du har vært og hvor du beveger deg*, (9) *hvilke nettsider du har besøkt/sett på*, (10) *bilder av deg*, og (11) *hva du har søkt etter på søkemotorer*. Svaralternativene rangeres fra *helt uviktig, lite viktig, litt viktig* til *veldig viktig*, i tillegg til *vet ikke* som jeg har fjernet. Det er med andre ord data på ordinalnivå som jeg velger å behandle som intervalldata, et metodisk valg som jeg har redegjort for tidligere.

Disse variablene har som fellesnevner at de omhandler personopplysninger som kan beskrives som *digitale fotavtrykk.* Nettsidebesøk og aktivitet på søkemotorer genererer digitale fotavtrykk som er verdifulle for ulike kommersielle aktører. Kategorien *bilder av deg* er ikke på samme måte handlingsdrevet, men bilder er ofte personlige og beskyttelsesverdige. Man

kan innvende at ikke alle bilder eksisterer digitalt, og at dette heller ikke er presisert i spørsmålet, men jeg vil hevde at å miste kontroll over bilder i liten grad var en reell frykt før disse i så stor grad ble digitaliserte. Å miste kontrollen over bilder du har fremkalt, og dermed eksisterer som et fysisk dokument, vil forutsette enten innbrudd i hjemmet eller en utro tjener i fotobutikken. Jeg velger derfor å tolke denne kategorien som et spørsmål om digitale fotografier.

Den siste variabelen som vil inngå i indeksen omhandler hvor man har vært og beveger seg i det fysiske rom. Jeg vil hevde at denne kategorien er beslektet med de tre andre i kraft av at stadig sterkere og mer kompakt prosessorkraft i bærbare enheter har muliggjort en mer hyppig og automatisert registrering av lokasjoner. Slik registrering kan skje ved hjelp av tradisjonelle overvåkningskameraer, men er stadig hyppigere en effekt av at apper på smarttelefonen får tilgang på lokasjonsdata for å kunne tilby mer effektive tjenester basert på din bevegelse i det fysiske rom (Datatilsynet 2014). Dermed har det skjedd en sammenkobling mellom de kommersielle tjenestetilbyderne og lokasjonsbasert overvåkning, ved hjelp av stadig mer sofistikerte smarttelefoner.

For å kunne bruke en additiv indeks som avhengig variabel er det viktig å teste den. Dette vil jeg gjøre i analysekapittelet i form av en faktoranalyse. Denne analysen vil altså gi empiriske indikasjoner på om de fire variablene nevnt ovenfor er en velfungerende indikator på begrepet *ønske om lovregulering av flyten av personopplysninger på nett*. Denne analysen vil altså innlede den andre analysedelen, og vil derfor ikke omtales mer her.

4.2.3 Bivariate analyser

Etter å ha opprettet indeksen vil jeg benytte denne som avhengig variabel i de påfølgende analysene som skal besvare den andre problemstillingen. Jeg vil begynne med å ta utgangspunkt i indeksens gjennomsnitt, og undersøke hvordan dette gjennomsnittet fordeler seg på de uavhengige variablene. Jeg vil på denne måten bygge opp analysen steg for steg, fra helt enkle univariate frekvensfordelinger til jeg ender opp med en multivariat regresjonsanalyse som inkluderer samtlige variabler.

De første uavhengige variablene jeg vil undersøke er de to *erfaringsvariablene.* Som jeg har drøftet tidligere vil jeg hevde at det er viktige nyanser mellom de to spørsmålene. Derfor vil jeg begynne med det mest generelle spørsmålet, *personopplysninger på avveie*, og gå videre

med spørsmålet som omhandler *uønsket bildepublisering*, som jeg har tolket som en mer konkret variant av samme problemstilling. Med utgangspunkt i indeksens gjennomsnitt vil jeg se på frekvensfordelingen på disse to, for å få en første, grov indikasjon på eventuelle sammenhenger. Jeg vil deretter gjennomføre samme type tabellanalyse av variablene kjønn, alder og utdannelse, igjen basert på gjennomsnittet av den opprettede indeksen. Disse bivariate analysene vil gi de første indikasjonene på hvilke variabler som påvirker ønsket om lovregulering av flyten av personinformasjon på nett.

4.2.4 Regresjonsanalyser

I den neste analysedelen vil jeg undersøke effekten de to erfaringsvariablene har på indeksen for holdning til lovregulering, ved hjelp av bi- og multivariate regresjonsanalyser. Jeg vil først undersøke effekten av de to erfaringsvariablene har på indeksen hver for seg, før jeg lar begge inngå i samme modell. Jeg vil hevde at det er hensiktsmessig å gjennomføre slike bivariate regresjonsanalyser, og ikke bare enklere korrelasjonsanalyser, fordi førstnevnte metode skiller mellom variabler som forklarer og variabler som blir forklart, mens enkle korrelasjonsanalyser kun avdekker sammenheng (Midtbø 2007, 73).

Videre vil jeg inkludere samtlige variabler, både erfaringsvariablene og de sosiodemografiske kontrollvariablene, i en multivariat, sekvensiell regresjonsmodell. Regresjonsanalyse kan gjennomføres for bivariate sammenhenger, slik gjør i den første modellen, men det er likevel denne analysemetodens evne til å håndtere multivariate forhold som er poenget med regresjonsanalyser. Dette innebærer at vi får muligheten til å «holde et antall uavhengige variabler konstante i den hensikt å se hvilken variabel eller hvilke variabler som påvirker den avhengige variabelen» (Hjerm og Lindgren 2011, 72/79).

Ifølge samme forfattere er det først og fremst to interessante ting en regresjonsanalyse kan avdekke. For det første kan modellen brukes til å forutsi utfall, eller effekter (Hjerm og Lindgren 2011, 74). Min analyse vil som nevnt ta sikte på å undersøke hvordan de uavhengige variablene kan predikere verdien på indeksen, som altså måler holdning til lovregulering av flyten av personopplysninger på nett. En regresjonsanalyse kan dermed predikere hvilken verdi på indeksen – hva slags holdning til lovregulering – en person vil ha, basert på en bestemt verdi på én av de uavhengige variablene. Dette fremgår i analysen som regresjonskoeffisienten, og denne tolkes som at hvis den uavhengige variabelen øker med ett nivå, øker verdien på indeksen med dette tallet.

I tillegg kan en regresjonsanalyse bidra til å forklare *hva* som påvirker den avhengige variabelen, ved å beregne determinasjonskoeffisienten, eller R^2. Dette tallet er et mål på modellens forklaringskraft, altså hvor mye av variasjonen på den avhengige variabelen som forklares av den eller de uavhengige variablene. Å etterstrebe en determinasjonskoeffisient opp mot 1 (altså 100 % forklaringskraft), altså jobbe bevisst for at modellen skal forklare så mye av variansen i den avhengige variabelen so mulig, er imidlertid ikke noe mål i seg selv (Hjerm og Lindgren 2011, 77), og bør ikke tillegges for stor betydning (Midtbø 2007, 89). Effekter er ofte interessante selv om den forklarte variasjonen ikke er kjempestor. I vår sammenheng er det åpenbart at grunnene til at ulike mennesker vektlegger viktigheten av lovregulering av personopplysninger er mange og varierte, utover de uavhengige variablene vi undersøker effekten av. Det ville vært rart om en slik holdningsvariabel kun var avhengig av de to erfaringsvariablene og de tre sosiodemografiske kontrollvariablene.

4.3 Reliabilitet, validitet og generaliserbarhet

Reliabilitet og *validitet* er to overordnede begreper som benyttes for å bedømme datakvaliteten i samfunnsvitenskapelige studier (Grønmo 2004, 220). Reliabilitet refererer til datamaterialets pålitelighet, mens validitet forstås som «i hvilken grad undersøkelsesopplegget egner seg til å samle inn data som er relevante for problemstillingene i en bestemt studie» (Grønmo 2004, 220 – 221).

Høy reliabilitet forutsetter at undersøkelsesopplegget og datainnsamlingen gir pålitelige data. Denne påliteligheten kommer til uttrykk ved at samme undersøkelsesopplegg gir identiske data ved ulike innsamlinger av data om de samme fenomenene (Grønmo 2004, 220). Høy validitet oppnås på den annen side ved at undersøkelsesopplegget egner seg for å samle inn data som er relevante for problemstillingen (Grønmo 2004, 221).

Disse to kategoriene kan sies å være delvis utfyllende kriterier for å vurdere kvaliteten i et undersøkelsesopplegg, men er samtidig delvis overlappende. Først og fremst kommer dette til uttrykk gjennom at høy reliabilitet er en forutsetning for høy validitet. Er undersøkelsesopplegget basert på data som ikke er pålitelige kan ikke et datamateriale være gyldig eller relevant for problemstillingen (Grønmo 2004, 221). Tilsvarende kan et datamateriale ha høy reliabilitet uten at validiteten nødvendigvis er høy, altså at datamaterialet er pålitelig, men lite egnet til å besvare problemstillingene (Grønmo 2004, 221).

Validitet er et mer omfattende og mindre presist mål for datakvalitet enn reliabilitet (Grønmo 2004, 231), og man kan skille mellom flere ulike typer validitet. Den enkleste formen for validitet, som både kan benyttes i kvantitative og kvalitative studer, kalles *åpenbar validitet,* og refererer til «trekk ved datainnsamlingen som er åpenbare for både forskeren selv og andre» (Grønmo 2004, 231). En vurdering av validiteten vil da handle om å vurdere hvor vidt «de innsamlede data er gode og treffende i forhold til studiens intensjoner» (Grønmo 2004, 231). *Definisjonsmessig validitet* er en vurdering som gjøres i kvantitative studier, og refererer til «forholdet mellom teoretiske og operasjonelle definisjoner av begreper» (Grønmo 2004, 232). Den teoretiske definisjonen sier altså noe om hva forskeren ønsker å studere, mens den operasjonelle definisjonen forteller noe om hva som faktisk blir studert (Grønmo 2994, 232).

Som jeg har diskutert i begynnelsen av dette kapittelet baserer jeg min oppgave på et datamateriale som allerede er samlet inn, av Opinion Perduco, et profesjonelt analyseselskap. En vurdering av denne oppgavens reliabilitet vil følgelig basere seg på et premiss om at dette selskapet besitter kompetanse med hensyn til datainnsamling som gir reliable data. Det er imidlertid viktig å understreke at holdninger til personvern konstant endres, blant annet i samspill med teknologiske, kulturelle og politiske utviklingstrekk. I den sammenheng er det et viktig poeng at undersøkelsen jeg baserer oppgaven min på ble gjennomført i kjølvannet av én av de mest omfattende overvåkingsskandalene i moderne tid, noe som sannsynligvis har preget svargivingen. Dermed kan det tenkes at samme undersøkelse vil gi noe endrede svar på et senere tidspunkt, når Snowden-saken har havnet mer i bakgrunnen av nyhetsbildet. På samme måte kan det også tenkes at å gjennomføre denne undersøkelsen rett etter et terroranslag kan påvirke respondentene til å avgi andre svar. For eksempel kan en slik traumatisk hendelse føre til at flere vurderer kriminalitetsbekjempelse som viktigere enn personvern.

Som jeg har argumentert for i delen om analysemetoder bidrar bruken av en indeks som avhengig variabel i kvantitative studier både til økt reliabilitet og validitet. En indeks gjør muligheten for tilfeldige feil mindre, og dermed øker reliabiliteten (Hjerm og Lindgren 2011, 34). Hvis for eksempel én av variablene har en spørsmålsstilling som kan misforstås av respondentene, minsker dennes påvirkningskraft sammenslått med andre variabler.

En sammenslåing av flere variabler representerer også en bedre operasjonalisering av et teoretisk begrep, noe som innebærer økt definisjonsmessig validitet (Hjerm og Lindgren

2011, 33). Summen av flere variabler vil med andre ord fange opp et bredere spekter av det samme begrepet enn en enkelt variabel kan.

Å basere seg på et datamateriale samlet inn av et profesjonelt analysebyrå på oppdrag av andre enn meg selv, innebærer også noen ulemper, som jeg har diskutert i begynnelsen av dette kapittelet. Én av disse ulempene er at Datatilsynet, som bestilte undersøkelsen, sannsynligvis har andre motiver og siktemål enn forskning. Det er sannsynlig at Datatilsynet i større grad ønsker å kartlegge sammenhenger og generelle tendenser, som i sin tur kan generaliseres til befolkningen som helhet. I tillegg er det nærliggende å tro at gjennomslag i media og oppmerksomhet rundt tematikken er viktig for Datatilsynet. I sammenheng med kvalitetsvurderinger av datamaterialet er det derfor grunn til å tro at en litt annen utforming av spørreskjemaet, med mer nøyaktig målenivå og større grad av standardiserte svaralternativer, ville økt datamaterialets reliabilitet. Som jeg har diskutert tidligere vil jeg likevel hevde at fordelene ved å basere seg på et slikt omfattende datamateriale veier mye tyngre enn ulempene.

Én åpenbar fordel ved å benytte dette datamaterialet er at jeg kan generalisere funnene til å gjelde hele populasjonen, som for denne undersøkelsen er den norske befolkningen, 15 år eller eldre. Statistisk generalisering bygger på sannsynlighetsteori og innebærer at forskjeller mellom utvalget og universet i prinsippet skyldes tilfeldigheter (Grønmo 2004, 86), og disse tilfeldighetene kan estimeres. Å basere oppgaven på det datamaterialet som jeg gjør representerer også på denne måten en stor fordel.

Igjen er det nødvendig å understreke at siden dette feltet i så stor grad endres kontinuerlig bør denne generaliseringen avgrenses til tidspunktet datainnsamlingen fant sted. Det er derfor grunn til å hevde at funnene fra denne undersøkelsen bør tolkes som et tidsbilde på holdninger til personvern i kjølvannet av Snowden-avsløringene.

5 Analyse og funn

Jeg vil nå gå videre med å anvende det metodiske opplegget skissert i forrige kapittel på datamaterialet. Jeg vil først gjennomføre bivariate krysstabellanalyser for å undersøke den første problemstillingen som tar sikte på å undersøke *sammenhengen mellom ulike holdninger til personvern*. Videre vil jeg ta for meg den andre problemstillingen, som vil undersøke om *personlige negative erfaringer med tap av kontroll over personopplysninger predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett*. Dette vil jeg gjøre ved hjelp av bi- og multivariate regresjonsanalyser med utgangspunkt i en additiv indeks som avhengig variabel. Funnene vil bli diskutert fortløpende i dette kapittelet, før en avsluttende og oppsummerende diskusjonsdel følger i neste kapittel.

5.1 Sammenheng mellom ulike holdninger

Den første problemstillingen tar altså sikte på å undersøke om det finnes en sammenheng mellom å være opptatt av personvern og (a) *villighet til å ta i bruk personvernkrenkende teknologi* og (b) *hvordan personvernet veies opp mot andre interesser på et overordnet nivå*.

Jeg vil begynne med å undersøke sammenhengen mellom graden av opptatthet av personvern og villighet til å benytte teknologi som på ulike måter kan sies å krenke personvernet, GPS-sporing av egne barn og Google-briller. Videre vil jeg sette det overordnede spørsmålet om grad av opptatthet av personvern opp mot konkrete, normative påstander hvor personvern veies opp mot andre interesser, henholdsvis *sikkerhet* og *bekvemmelighet*. Til sammen vil denne analysedelen danne utgangspunkt for en diskusjon om ulike måter å forstå fenomenet som av flere har blitt kalt *personvernparadokset* (Barnes 2006, Norberg, Horne og Horne 2007, 101).

Flere ulike studier har nemlig pekt på at holdninger til personvern ikke nødvendigvis gjenspeiles i handlinger (for eksempel Fox et al. 2000, Nissenbaum 2010, 104, Barnes 2006, Norberg, Horne og Horne 2007, 101). Eksempelvis proklamerer vi viktigheten av et robust personvern samtidig som vi velvillig gir fra oss personopplysninger i bytte mot rabattkort i butikker og gratis emailtjenester. Å forstå denne inkonsistensen som et personvernparadoks er etter mitt syn en noe overflatisk tilstandsrapport. Som jeg har diskutert i teoridelen er det flere medvirkende årsaker til at en slik beskrivelse bør nyanseres. Den første grunnen kan

oppsummeres som *teorien om kontekstuell integritet* (Nissenbaum 2010). Hva som oppleves som personvernkrenkende vil variere mellom blant annet samfunn, historiske tider og enkeltindivider, og de fleste er mer opptatt av at personinformasjon flyter riktig, enn at informasjonen er hemmelig (Nissenbaum 2010, 2). Å forstå personvern som en absolutt rettighet er ifølge en slik forståelse inkompatibelt med faktiske forhold, og overser fullstendig konteksten informasjonen avgis i.

For det andre er det mye som tyder på at mange av handlingene som innebærer å gi fra seg personopplysninger ikke forstås av brukerne, særlig når disse er standardiserte tjenesteavtaler på nett, hvor brukeren godtar en avtale i bytte mot gratis tjenester eller innhold. Dermed vil en forutsetning for å forstå denne inkonsistensen som et paradoks falle bort. Hvis man ikke har begrep om hva konsekvensene av å avgi informasjon er, eller simpelthen ikke har kompetanse nok til å tilegne seg denne kunnskapen, er det en snarvei å kalle det et paradoks at de samme menneskene har sterke meninger om viktigheten av et robust personvern. Flere undersøkelser som jeg har redegjort for i teorikapittelet antyder at dette er tilfelle (for eksempel Solove 2004, 82, Shapiro 1999, 162, Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow 2003, 19, Smith 2014, Schwartz 1999, 1684 – 1685).

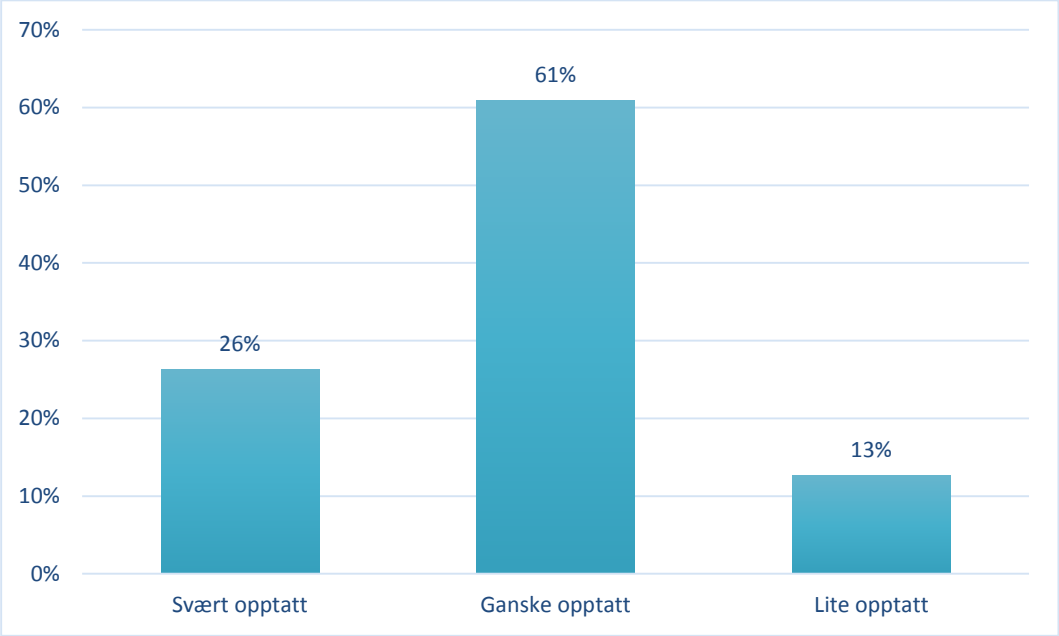
Jeg mener at disse første analysene er hensiktsmessige for å undersøke om de samme tendensene kan gjenfinnes i mitt datamateriale, og vil bruke disse funnene som utgangspunkt for å diskutere de ulike teoretiske perspektivene.

Er personvern viktig?

Utgangspunktet for krysstabellanalysene som følger vil være det første spørsmålet i undersøkelsen, som spør om den overordnede personvernbevisstheten[8]. Respondentene fordeler seg på følgende måte på dette spørsmålet:

[8] Spørsmål 1. I hvilken grad er du opptatt er du av personvern?

Figur 6.1: *I hvilken grad er du opptatt er du av personvern*



N = 1501 Svært opptatt: N=395, Ganske opptatt: N=915, Lite opptatt: N=191

Som figur 6.1 viser oppgir den største andelen å være *ganske opptatt* av personvern, mens omtrent en fjerdedel velger alternativet *svært opptatt*. Litt over én av ti oppgir å være *lite opptatt av personvern*. Omkring ni av ti velger altså alternativene *svært* eller *ganske opptatt av personvern*, noe som vitner om at personvern oppfattes som viktig.

Disse tallene samsvarer i stor grad med kategoriseringen gjort av befolkningsundersøkelsen *The Harris Poll*, et selskap som utarbeider markedsanalyser, i samarbeid med professor Alan Westin, som regnes som opphavsmannen bak skillet mellom personvern og personopplysningsvern (Solove 2008, 24, Selmer og Blekeli 1977, 16). Denne rapporten deler befolkningen i tre basert på graden av viktighet personvern gis. 26 prosent kategoriseres som personvernfundamentalister, 64 prosent som personvernpragmatikere og 10 prosent som ubekymrede (Taylor 2003). Denne fordelingen er med andre ord slående lik funnene presentert ovenfor. Det er imidlertid ikke helt uproblematisk å sette likhetstegn mellom *ganske opptatt av personvern* og *personvernpragmatikere*. Den siste kategorien antyder et reflektert forhold til problematikken, og en grad av veiing av interesser, noe å være «ganske opptatt av» ikke kan sies å gjøre.

Økt grad av personvernbevissthet

46 prosent oppgir i Personvernundersøkelsen at de har blitt *mer opptatt av personvern* de siste to, tre årene, mens 49 prosent oppgir å være *like opptatt av personvern*[9]. Fordelingen representerer en endring fra en undersøkelse Statistisk Sentralbyrå gjennomførte på oppdrag av Datatilsynet i 1997, hvor samme spørsmål ble stilt (Gulløy 1997, 29). Her oppga 22 prosent å være *svært opptatt*, 55 prosent *ganske opptatt* og 23 prosent *lite opptatt av personvern*. Gruppen som oppgir å være *lite opptatt av personvern* er med andre ord halvert i figur 6.1 sammenlignet med funnene i undersøkelsen fra 1997, noe som kan sies å vitne om en klar forskyving i retning av større interesse for personvern. Denne endringen i retning økt bevissthet rundt personvern er også noe rapporten fra Harris Interactive påpeker (Taylor 2003, 1).

Denne endringen kan komme av flere ting. For det første lever vi i dag mer digitale liv enn tidligere, noe som sannsynligvis har økt følelsen av sårbarhet med hensyn til kontroll over personopplysninger. Den økte digitale tilstedeværelsen har også ført med seg medieoppmerksomhet rundt tidligere ukjente farer som identitetstyveri og hacking. Selv om personvern opptok folk før internettets tidsalder er det grunn til å tro at den økende digitale tilstedeværelsen har medbrakt en større grad av personvernbevissthet.

I tillegg er det viktig å nevne at undersøkelsen jeg baserer oppgaven på ble gjennomført i kjølvannet av en av historiens største overvåkingsskandaler. Edward Snowdens avsløring av den amerikanske etterretningsorganisasjonen NSAs overvåkingspraksis synliggjorde både amerikanske myndigheters evne og vilje til å registrere enorme mengder informasjon om borgere uten bånd til terrorisme eller annen type kriminalitet (Gellman og Poitras 2013, Greenwald 2013). En fersk undersøkelse fra PEW Research Centre viser for eksempel at én av tre amerikanere har tatt grep for å beskytte sitt privatliv som en direkte følge av Snowden-avsløringene (Rainie og Madden 2015, 4). På samme måte oppgir 59 prosent i Personvernundersøkelsen at Snowden-avsløringene ikke har påvirket deres handlinger. Selv om denne gruppen er en majoritet innebærer det at Snowden-avsløringene har påvirket handlingene til 41 prosent i undersøkelsen. Snowden-avsløringene blottla en overvåkingspraksis som synliggjorde hvor lite kontroll den enkelte internettbruker har over

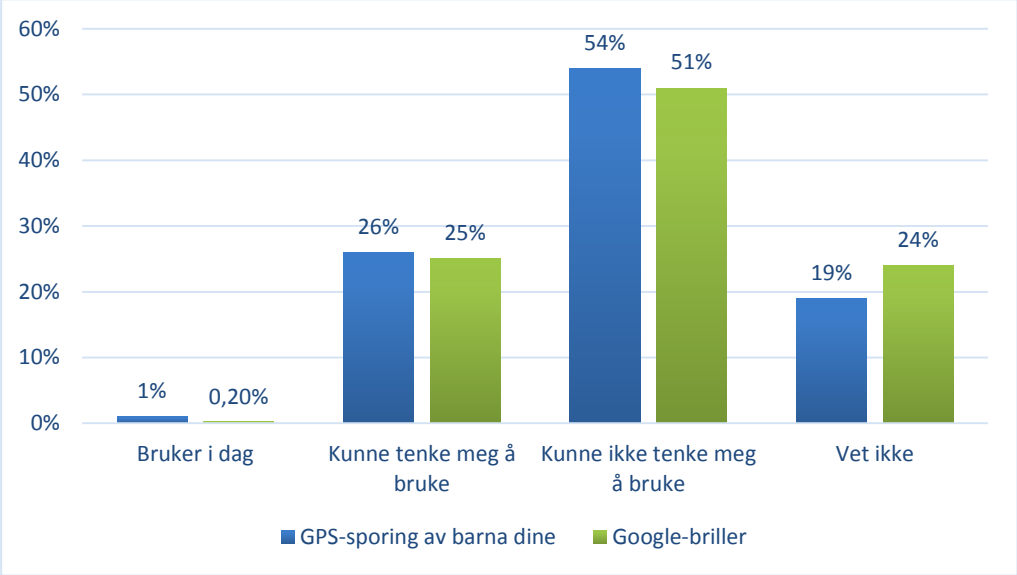
[9] Spørsmål 2. Har du blitt mer eller mindre opptatt av personvern de siste to-tre årene?

informasjonen som avgis på internett, og det kan hevdes at mange har endret atferd som en direkte følge av dette.

5.1.1 Personvern og ny teknologi

Jeg vil nå flytte fokus fra overordnede personvernholdninger til spørsmål om villighet til å ta i bruk *GPS-sporing av egne barn* og *Google-briller*. Dette er eksempler på teknologi og tjenester som på ulikt vis legger press på personvernet. Som jeg har redegjort for i metodekapittelet er GPS-sporing av barn en åpenbar personvernkrenkelse av barnets integritet og autonomi, mens Google-briller blant annet representerer problemer med tanke på registrering av uvitende tredjeparter i det offentlige rom.

Figur 6.2: *GPS-sporing av barna dine* og *Google-briller*



N=1501

Villigheten til å benytte de to tjenestene er jevnt over lik, som vist i figur 6.2. En majoritet kan *ikke* tenke seg å benytte slik teknologi. Omkring en fjerdedel kan tenke seg å benytte tjenestene, mens det også er en betydelig andel som svarer *vet ikke*. Det er nærliggende å tro at dette kan forklares med at teknologien er ukjent for respondentene, og at de dermed velger å ikke ta stilling. Google-briller er for eksempel et produkt som ennå ikke er lansert på det norske markedet, og dermed forutsetter det å ta stilling til bruken at man har lest om det. Den forsvinnende lille andelen som faktisk bruker teknologien bekrefter på et vis at dette er ukjente problemstillinger for de fleste, og innebærer også at spørsmålet må tolkes som et holdningsspørsmål. Hadde andelen som benyttet teknologien vært stor kunne muligens

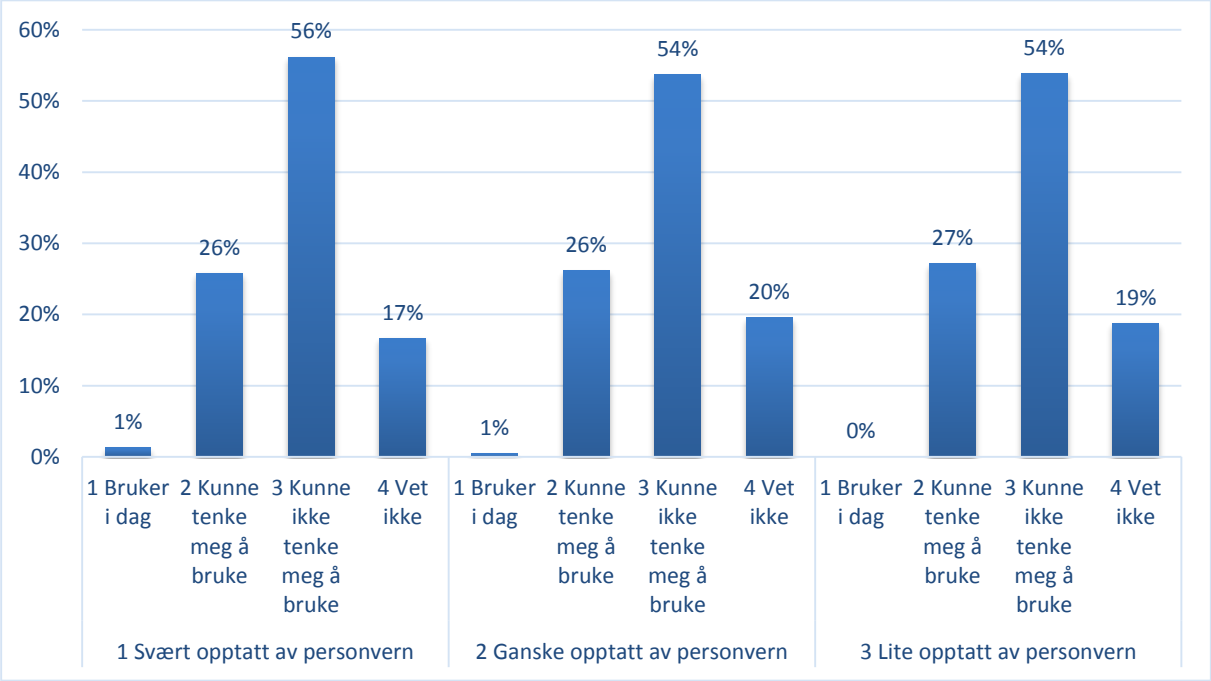
funnene fra krysstabellanalysen blitt tolket på en annen måte, siden funnene da ville sagt noe om faktiske handlinger.

Det er imidlertid også en ikke ubetydelig andel av respondentene som kan tenke seg å benytte teknologien, omkring én av fire i begge eksemplene. Det er imidlertid viktig å påpeke at det sannsynligvis ligger ulik motivasjon til grunn for dette ønsket. Å GPS-spore barn vil for de fleste være et tiltak for å holde barnet trygt, mens bruk av Google-briller i større grad handler om bekvemmelighet, og har sannsynligvis en grad av teknologisk nysgjerrighet knyttet til seg. I begge tilfeller ligger det sannsynligvis en interesseavveiing bak et slikt ønske, hvor gevinsten ved å ta i bruk tjenestene spiller inn og veies opp mot eventuelle kostnader. Denne interesseavveiingen vil diskuteres mer inngående i neste avsnitt.

Bivariate analyser - paradoksal bruk av teknologi?

Den univariate analysen i figur 6.1 viser altså en generelt høy grad av opptatthet av personvern. Hele ni av ti oppgir å være *svært* eller *ganske opptatt av personvern*, mens kun én av ti oppgir å være *lite opptatt av personvern*. Videre viser figur 6.2 og 6.3 at en majoritet *ikke* kan tenke seg å benytte *GPS-sporing av egne barn* og *Google-briller*, mens omtrent en fjerdedel kan tenke seg det i begge figurene. Jeg vil nå krysstabulere den overordnede holdningsvariabelen med de to variablene som omhandler bruk av personverntruende teknologi, for å besvare problemstillingen *finnes det en sammenheng mellom hvor opptatt man er av personvern og hvor villig man er til å ta i bruk personvernkrenkende teknologi?* Det er nærliggende å tro at en høy grad av opptatthet av personvern fører til en større motstand mot teknologi som krenker personvernet. Figuren under viser variabelen *GPS-sporing av barna dine*, og hvordan svarene fordeler seg på de ulike «personverngruppene»:

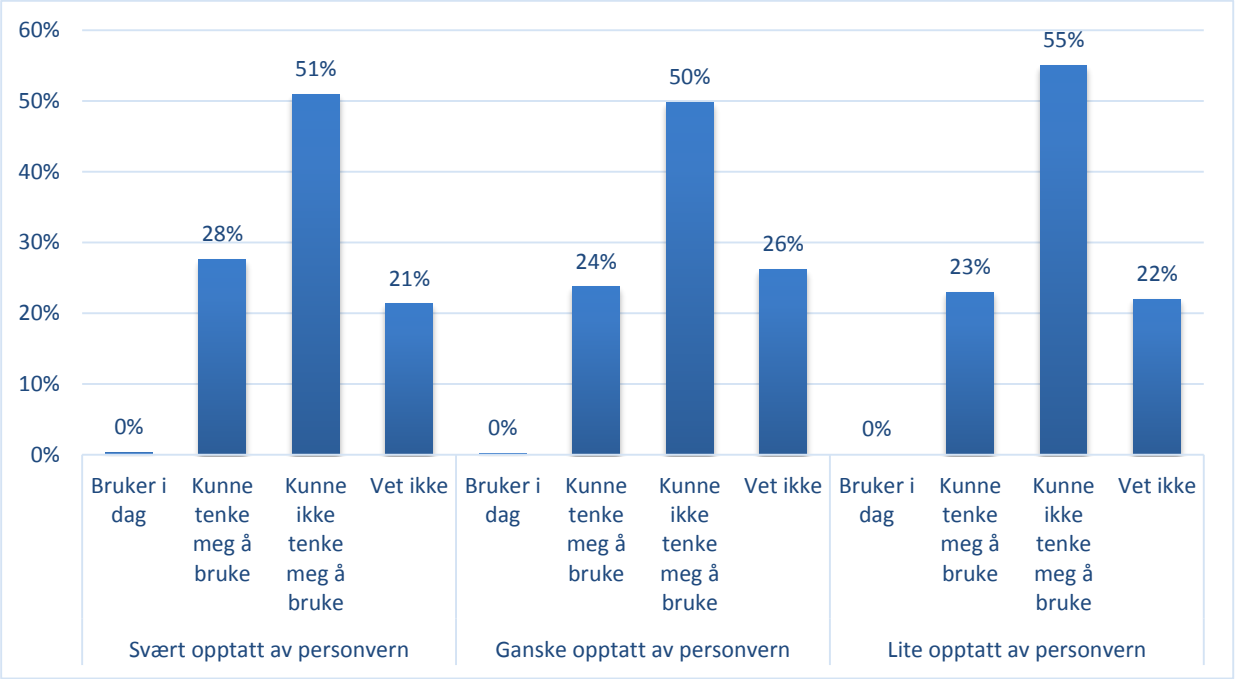
Figur 6.3: *GPS-sporing av barna dine* krysstabulert med *I hvilken grad er du opptatt av personvern.*



Det hadde som nevnt vært nærliggende å tro at å være svært opptatt av personvern innebærer en motvilje mot å GPS-spore egne barn, et tiltak som i stor grad går utover barnets integritet og selvstendighet. En slik sammenheng finnes imidlertid ikke, som figur 6.3 viser. I overkant av halvparten i hver kategori motsetter seg et slikt tiltak, omkring én av fire kan tenke seg å bruke slik teknologi, mens i underkant av én av fem oppgir «vet ikke». Det er altså ingen markante forskjeller mellom de ulike personverngruppene og villighet til å benytte GPS-sporing av egne barn.

Den samme tendensen finner vi når spørsmålet gjelder Google-briller. Dette er et eksempel på såkalt kroppsnær teknologi, som brukeren bærer med seg som et par briller. Disse er utstyrt med sensorer, GPS, kamera og andre egenskaper moderne smarttelefoner er utstyrt med, og brukeren kan dermed få tilgang til alle disse funksjonene uten å ta fram telefonen. Fra et personvernperspektiv er slik teknologi problematisk, da de muliggjør registrering av intetanende tredjeparter, uten at disse er klar over det. En sentral egenskap som skiller Google-briller fra en smarttelefon, som i stor grad er utstyrt med den samme teknologien, er at brillene ikke må tas fram for å brukes, men til enhver tid er klargjort for bruk. Dette medfører for eksempel at personer som ikke nødvendigvis vil bli tatt bilde av frarøves muligheten til å bli gjort oppmerksom på registrering, all den tid den fysiske handlingen med å holde smarttelefonen foran objektet ikke lenger er nødvendig.

Figur 6.4: *Google-briller* krysstabulert med *I hvilken grad er du opptatt av personvern.*



Som vi kan lese av figur 6.4 kan omkring én av fire tenke seg å bruke Google-briller i alle «personverngruppene». Omtrent halvparten er uvillige, mens litt over én av ti kan tenke seg å gjøre det. Det er verdt å merke seg at en *større* andel blant de som oppgir å være *svært opptatt av personvern* kan tenke seg å bruke Google-briller. Graden av opptatthet av personvern innebærer tilsynelatende ikke en økt motvilje mot å ta i bruk teknologi som er problematiske fra et personvernperspektiv.

Denne tendensen kan gjenfinnes i alle de andre spørsmålene. Å være svært opptatt av personvern innebærer ikke motvilje mot å ta i bruk teknologi som på ulike måter er personverntruende. Jeg har valgt ut to av teknologiene og tjenestene det spørres om, og de ulike tjenestene har ulik oppslutning med tanke på villighet til å ta de i bruk. For eksempel kan rundt tre av fire tenke seg å benytte GPS-sporing av eldre eller andre familiemedlemmer med spesielle omsorgsbehov, mens kun 13 prosent kan tenke seg å gjøre opptak av egne telefonsamtaler (Datatilsynet 2013). Denne variasjonen kan forklares med at samtlige tjenester det spørres om har en åpenbar gevinst for brukeren, og hvordan disse veies opp mot personvernet varierer. Hovedpoenget i denne sammenhengen er imidlertid ikke den generelle villigheten, men hvor vidt denne påvirkes av graden av opptatthet av personvern. Det gjør den ikke.

En fellesnevner for alle disse teknologiene er som nevnt at de fyller en konkret, ofte praktisk funksjon, og at utfordringene knyttet til personvern på mange måter er en bieffekt av disse. I eksempelet med GPS-sporing av barn er det for eksempel åpenbart at en slik teknologi vil øke foreldrenes mulighet til å komme barnet raskt til unnsetning, hvis noe skulle hende, og gir foreldrene mulighet til å spore opp barnet, skulle det forsvinne. Spørsmålet representerer altså en interesseavveining mellom *personvern* og *sikkerhet*, og det kan hevdes at respondentene vurderer fordelene ved teknologien relatert til sikkerhet er større enn ulempene relatert til personvern. Når det gjelder Google-briller er det nærliggende å tro at verdien ligger i bekvemmeligheten de tilbyr, samt at å anskaffe nytt teknologisk utstyr ofte har et element av statusmessig verdi.

Dette er i tråd med Nissenbaums syn på *personvern som en kontekstavhengig rettighet* (2010), og det er grunn til å hevde at slik teknologi ikke nødvendigvis framstår som personverninngripende for de det gjelder – i det minste ikke for foreldrene som utstyrer barna med sporingsteknologien. Dette elementet – at teknologien muliggjør personvernkrenkelse av *andre individer* – kan også bidra til å forklare hvorfor graden av opptatthet av personvern ikke påvirker villigheten til å benytte teknologien. I hvilken grad respondentene reflekterer over de personvernkrenkende aspektene ved teknologien sier svargivingen ingenting om. Siden undersøkelsen omhandler personvern er det likevel grunn til å anta at dette aspektet er vurdert.

5.1.2 Personvern veid opp mot andre interesser

Den første analysen viste altså ingen sammenheng mellom graden av opptatthet av personvern og villighet til å benytte tjenester og teknologi som på ulikt vis er personvernkrenkende. Jeg har argumentert for at det implisitt i spørsmålet om å ta i bruk ny teknologi ligger en interesseavveiing. Jeg vil nå gå videre med å sammenligne den samme overordnede holdningsvariabelen – i hvilken grad er du opptatt av personvern – med konkrete utsagn som eksplisitt setter personvern opp mot andre interesser.

En av disse interessene er sikkerhet. Denne interesseavveiingen er en nødvendig og akseptert del av å leve i en rettsstat, og er ofte sentral når personvern løftes opp i politiske debatter. På mange måter er dette en type interesseavveiing som er løftet over hodene på enkeltindividene, og i stor grad gjøres av politiske beslutningsmyndigheter på nasjonalt nivå, for eksempel i spørsmålet om hvilke verktøy politiet skal kunne benytte seg av for å bekjempe kriminalitet.

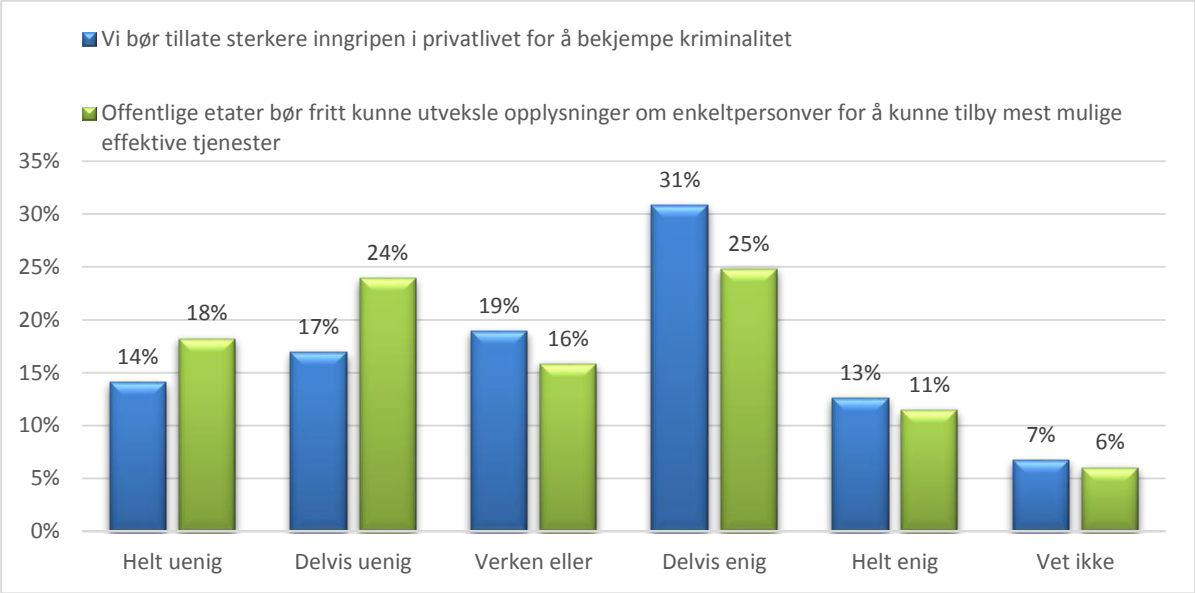
Det er også sannsynlig at denne interesseavveiingen preges av følelser og medieoppmerksomhet relatert til terrorisme og overgrep mot barn.

Å vurdere personvern opp imot sikkerhet er imidlertid langt ifra den eneste interesseavveiingen vi gjør. En annen interesse som ofte kommer i konflikt med personvernet er bekvemmelighet, det som på engelsk heter *convenience*. Dette begrepet kan innebefatte en hel rekke verdier og interesser, fra funksjonelle kommunikasjonstjenester og sosiale nettsamfunn til effektiv tjenesteformidling fra NAV og fastlegesystemet og hjelpemidler for pleietrengende. For eksempel har det nylig blitt standard med elektroniske resepter. Fra et bekvemmelighetsperspektiv er det åpenbart en forbedring å slippe papirresepten og bare vise legitimasjon på apoteket. Fra et personvernperspektiv innebærer det imidlertid at informasjon om medisinene dine eksisterer et sted utenfor din rekkevidde, og at du er nødt til å stole på at den er trygg der. Bruk av Google-briller og andre former for kroppsnær teknologi representerer også bekvemmelighetsinteresser. Å frembringe mer effektivitet har vært en betydelig drivkraft bak innsamling, lagring og sammenstilling av personinformasjon (Nissenbaum 2010, 109).

I det følgende vil jeg ta utgangspunkt i to normative påstander som eksplisitt setter personvern opp mot disse to motstridende interessene, *sikkerhet*[10] og *bekvemmelighet*[11]:

[10] 28.7: Vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet
[11] 28.4: Offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulig effektive tjenester

Figur 6.5: *Vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet* og *Offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulige effektive tjenester*



Den univariate frekvensfordelingen presentert i figur 6.5 viser at de to spørsmålene representerer en interesseavveiing uten et tydelig preferert alternativ. Tallene indikerer at det ikke er åpenbart hvilken interesse, personvern eller henholdsvis *sikkerhet* og *bekvemmelighet*, som bør veie tyngst, noe den relativt store andelen som velger de mer nøytrale svaralternativene bekrefter.

Tyngdepunktet i spørsmålet om offentlige etater, altså *bekvemmelighetsavveiingen*, ligger på svaralternativet *delvis enig*, mens det i spørsmålet om kriminalitetsbekjempelse, *sikkerhetsavveiingen*, er en omtrent like stor andel som sier seg *delvis enig* og *delvis uenig*. Det er også verdt å peke på at respondentene i større grad sier seg helt eller delvis enige i at vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet enn at offentlige etater fritt bør kunne utveksle personopplysninger. Dette er ikke relevant for min undersøkelse, men antyder at kriminalitetsbekjempelse vurderes som en viktigere interesse enn bekvemmelighet, her eksemplifisert gjennom effektiv tjenesteformidling fra offentlige etater.

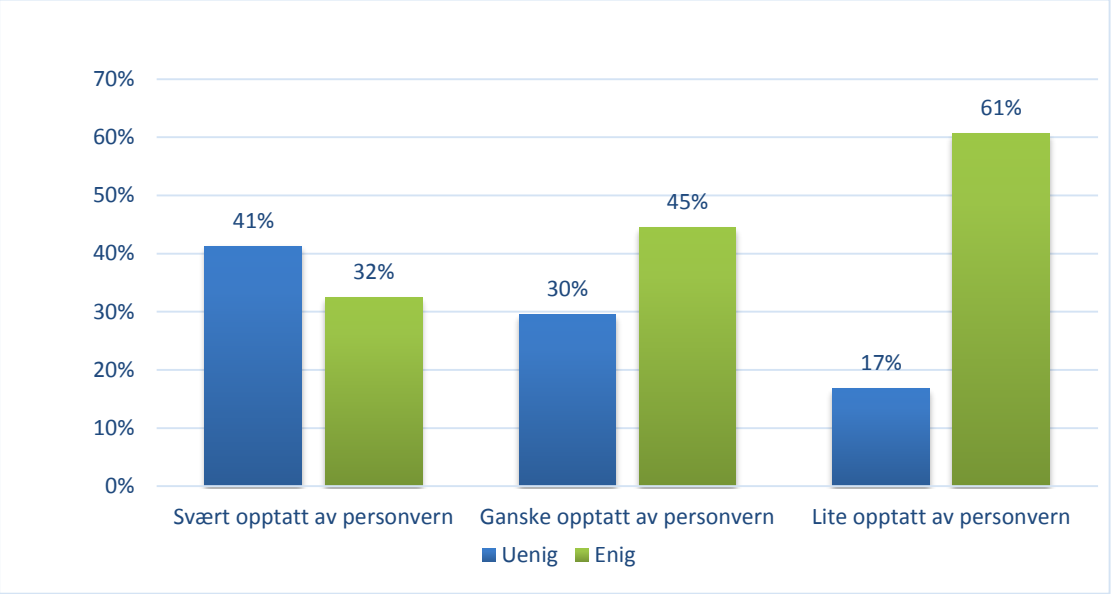
Det er også verdt å peke på at Personvernundersøkelsen viste at 85 % har stor eller noe tillitt til politiet, mens kun 65 % har stor eller noe tillit til NAV (Datatilsynet 2013). Tilliten til korrekt bruk av opplysninger som samles inn, det som i spørsmål 28.7 kalles *sterkere inngripen i privatlivet*, kan være med å spille inn når man skal vurdere personvern opp mot andre interesser, og er i tråd med Nissenbaums teori om *korrekt informasjonsflyt*. Har man stor tillit til hvordan informasjonen behandles er man mer villige til å oppgi den, særlig hvis målet for innsamlingen fremstår som viktig.

Bivariate analyser – personvern veid opp mot andre interesser

Jeg vil nå gå videre med å krysstabulere de to variablene som setter personvern opp mot andre verdier med den overordnede holdningsvariabelen *i hvilken grad er du opptatt av personvern*. Dette vil hjelpe meg med å belyse den andre delen av den første problemstillingen, *finnes det en sammenheng mellom hvor opptatt man er av personvern og hvordan man veier personvernet opp mot andre interesser på et overordnet nivå*. I analysene under har jeg slått sammen svarene i to enighetsgrupper – *helt* eller *delvis enig* på den ene siden, *helt* eller *delvis uenig* på den andre. I tillegg har jeg fjernet *vet ikke*. Fordelen med en slik oppdeling er at et mer tydelig bilde tegner seg med hensyn til hvilken side av skalaen tyngdepunktet ligger. Ulempen er selvfølgelig at noen nyanser går tapt:

Personvern kontra sikkerhet

Figur 6.6: *Vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet*, dikotome variabler krysstabulert med *i hvilken grad er du opptatt av personvern*



Resultatene i figur 6.6 skiller seg merkbart fra funnene i analysene som undersøkte sammenhengen mellom personvernholdninger og villighet til å ta i bruk personvernkrenkende teknologi. Vi kan observere en tydelig tendens til at graden av opptatthet av personvern har sammenheng med holdningen til spørsmålet om hvor vidt vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet. Omtrent dobbelt så mange av de som oppgir å være *lite opptatt av personvern* sier seg enige i påstanden enn de som *er svært opptatt av personvern*. Det er en tydelig retning som viser at mange flere av de som er svært opptatte av

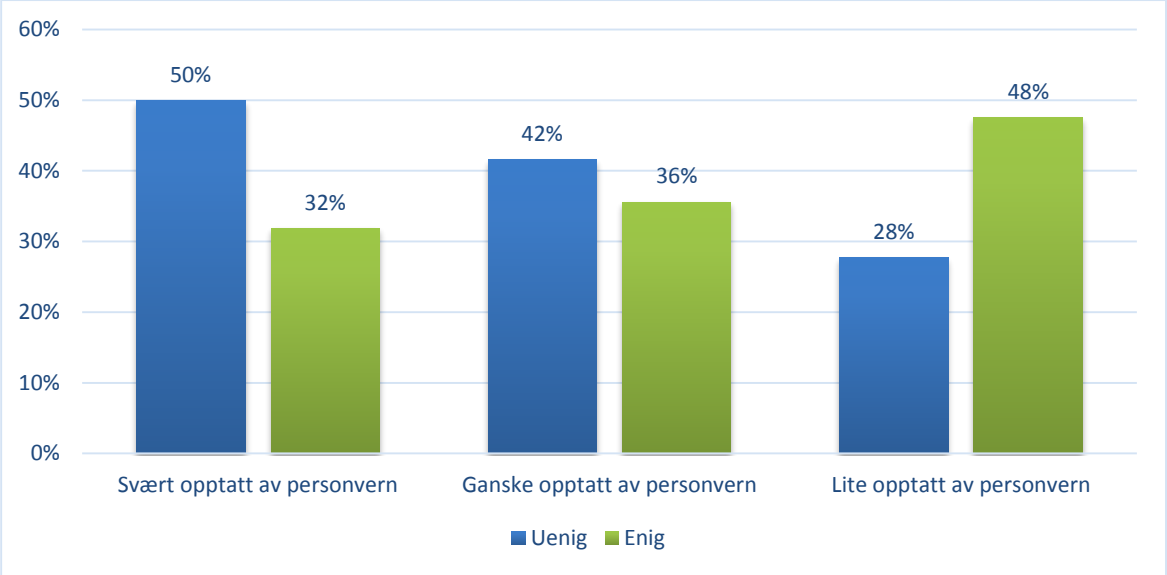
personvern motsetter seg sterkere inngripen i privatlivet for å bekjempe kriminalitet. At de som oppgir å være lite opptatt av personvern i større grad tar stilling, altså ikke velger *verken eller* eller *vet ikke*, kan muligens også forklares med at å være opptatt av personvern innebærer å anerkjenne den uten tvil vanskelige interesseavveiingen som ligger i utsagnet.

Bruken av dikotome variabler innebærer som nevnt at svargivingen fremstår som polarisert, og dermed at potensielt interessante nyanser går tapt. For eksempel er det verdt å nevne at svarene i kategorien *ganske opptatt av personvern* i større grad er konsentrert rundt midten, der de andre to kategoriene tenderer mot å oftere være *helt enig* eller *uenig*.

Personvern kontra bekvemmelighet

Den bivariate analysen ovenfor viste altså en klar sammenheng mellom å være opptatt av personvern, og å motsette seg inngripen i privatlivet for å bekjempe kriminalitet. Det neste utsagnet jeg vil ta for meg omhandler interesseavveiingen mellom personvern og effektive tjenester, som faller inn under samlebegrepet jeg har kalt *bekvemmelighet*. Å leve i en velferdsstat innebærer at personopplysninger om deg eksisterer i ulike registre, noe som er en forutsetning for at befolkningen blant annet kan motta gratis helsetjenester og utdanning. Disse registrene var utgangspunktet da Alan Westin skilte ut personopplysningsvern fra andre personvernkategorier (Westin 1970, 158). Disse personopplysningene er imidlertid ikke registrert samme sted. Fastlegen har ikke automatisk tilgang til sakspapirer fra NAV, Lånekassen har ikke innsyn i pasientjournaler. En enorm sammenstilling av all informasjon som eksisterer kunne imidlertid sannsynligvis gjøre tjenestetilbudet mer effektivt, samtidig som sammenstillingen av denne informasjonen også vil innebære at individet er mer sårbart, fra et personvernperspektiv. Å arbeide for å gjøre slikt tjenestetilbud mer effektivt har også vært en betydelig drivkraft bak innsamling, lagring og sammenstilling av personinformasjon (Nissenbaum 2010, 109).

Figur 6.7: *Offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulige effektive tjenester*, dikotome variabler krysstabulert med *I hvilken grad er du opptatt av personvern*



Figur 6.7 viser resultatene av den bivariate analysen. På samme måte som i forrige analyse har jeg sammenstilt alternativene *helt* og *delvis uenig* og *helt* og *delvis enig*, for å få et mer oversiktlig bilde av hvordan svarene fordeler seg. Halvparten av de som er *svært opptatt av personvern* motsetter seg slik informasjonsdeling, mot litt over en fjerdedel av de som er *lite opptatt av personvern*. I gruppen som er *ganske opptatt av personvern* er andelen som er *uenig* litt større enn *enig*, men forskjellen er ikke veldig stor. Det er en tydelig retning som antyder at villighet til å kompromisse med personvern for å oppnå mest mulig effektive tjenester henger sammen med graden av opptatthet av personvern.

Figur 6.6 og figur 6.7 har åpenbare likheter. De som er *svært opptatt av personvern* motsetter seg i større grad inngripen i privatlivet for å bekjempe kriminalitet og informasjonsutveksling mellom offentlige etater for å oppnå effektive tjenester, enn de som er *lite opptatt av personvern*. I begge figurene er forskjellene mellom de som er *lite opptatt av personvern* og *svært opptatt av personvern* markante. De som oppgir å være *ganske opptatt av personvern* plasserer seg som forventet i begge figurene et sted mellom de to ytterpunktene.

En interessant forskjell mellom de to figurene er at andelen som ikke tar stilling og velger alternativene *vet ikke* eller *verken eller* er minst blant de som er lite opptatt av personvern i figur 6.6, som omhandler personvern kontra *sikkerhet*, og størst i samme gruppe i figur 6.7, som omhandler personvern kontra *bekvemmelighet* Dette kan antyde at den første interesseavveiingen oppleves som enklere å vurdere, mens den andre interesseavveiingen

forutsetter en grad av kunnskap om personvern for å kunne ta stilling til. Det kan også tenkes at sikkerhet, herunder også bekjempelse av terrorisme, oppleves som så viktig at personvernet må vike, mens effektiv tjenesteformidling fra NAV ikke gjør det. Forskjellene er imidlertid ikke markante.

5.1.3 Oppsummering

Holdninger til personvern kan altså sies å påvirke hvordan man vurderer personvern opp imot konkurrerende interesser, når disse er presentert som normative påstander på et overordnet nivå. Det er en interessant observasjon at holdninger til personvern i så stor grad spiller inn på de overgripende interesseavveiingene, samtidig som de ikke påvirker villighet til å ta i bruk teknologi som går på akkord med disse prinsippene, som jeg viste i den første analysen.

Det kan være flere grunner til at det er slik. For det første kan det tenkes at verdien av teknologien det spørres om, GPS-sporing av egne barn og Google-briller, vurderes som større enn ulempene relatert til personvern. For det andre sier ikke svargivingen noe om i hvor stor grad de problematiske aspektene fra et personvernperspektiv vektes i forhold til de andre verdiene. Kanskje er teknologi som nærmest vil garantere at barnet ditt ikke blir borte, uten tvil de fleste foreldres verste mareritt, så forlokkende at personvernhensyn ikke engang vurderes? I tillegg rammer ikke GPS-sporing av barn personvernet til personen som svarer på spørsmålet, men en tredjeparts, i likhet med hva tilfellet er for Google-briller.

Det er mulig å argumentere for at å være barn, altså umyndig, innebærer at man uansett ikke har fullstendig autonomi, og dermed er ikke GPS-sporing nødvendigvis noe mer krenkende enn alle de andre avgjørelsene foreldre konstant tar på sine barns vegne. Jeg vil imidlertid hevde at å forstå barndom som en tilstand som rettferdiggjør alle tenkelige former for kontroll er et blindspor. Snarere er det å være barn en prosess hvor man er avhengig av foreldrene, samtidig som man konstant søker løsrivelse og selvstendighet. GPS-sporing er et middel som gjør denne løsrivingsprosessen vanskeligere for barnet, da det å vite at foreldrene vet hvor du er til enhver tid påvirker den naturlige prosessen med utforsking og selvstendiggjøring. På den annen side kan man argumentere for at slik teknologi muliggjør at barnet kan bevege seg lengre unna hjemmet, siden foreldrene uansett har kontroll over hvor det befinner seg, og dermed føre til mer selvstendiggjøring.

Når det gjelder Google-briller er det ikke nødvendigvis slik at de personvernkrenkende aspektene ved slik teknologi overhode vurderes. Medieoppmerksomhet rundt slike teknologiske nyvinninger fokuserer ikke nødvendigvis på disse aspektene, og siden Google-briller ennå ikke er lansert på det norske markedet vil personers holdninger til disse i stor grad basere seg på informasjon fra medier. I tillegg er ikke Google-briller personvernkrenkende i seg selv, men de har potensiale til å være det. Dette er en viktig presisering, for det innebærer at man kan vurdere de personverntruende aspektene ved teknologien, men likevel konkludere med at ansvarlig bruk ufarliggjør dem. For eksempel kan det godt tenkes at mange vil avstå fra å benytte seg av muligheten til å ta bilder av intetanende tredjeparter selv om det er mulig, basert på en personlig vurdering av en slik handling. På et overordnet nivå er det like fullt liten tvil om at jo flere som har mulighet til å benytte slik teknologi til å krenke andres personlige integritet, jo flere kommer til å gjøre det.

Det kan også tenkes at de normative utsagnene som den andre analysedelen baserer seg på fremstår som mer prinsipielt viktige for samfunnsutviklingen som helhet, enn spørsmålene om teknologi og tjenester. Å ta i bruk slik teknologi innebærer som nevnt også at man selv kan kontrollere bruken av det, og kanskje også begrense de personvernkrenkende egenskapene. I tillegg kan det spille inn at den umiddelbare gevinsten med å ta i bruk teknologien det spørres om oppleves som stor, mens et mer effektivt forvaltningssystem oppleves som en diffus og uhåndgripelig gevinst. Å ønske mer effektive tjenester fra det offentlige forutsetter også at man mener det eksisterer et behov for mer effektivitet i den offentlige sektor, noe ikke nødvendigvis alle mener. Har du for eksempel aldri stått i kø for å få levert et skjema for uføretrygd på det lokale NAV-kontoret, mens alle tjenester det offentlige har ytt har vært gode, vil muligens de personverntruende aspektene veie tyngre enn hvis du har svært negative erfaringer med det offentlige tjenestetilbudet.

Oppsummert viser funnene altså ingen sammenheng mellom å være opptatt av personvern og villighet til å benytte personvernkrenkende teknologi. Graden av opptatthet av personvern har ikke sammenheng med holdninger til å ta i bruk teknologi og tjenester som indirekte går på akkord med personvernprinsipper. Krysstabuleringen mellom graden av personvernbevissthet og de normative påstandene som eksplisitt setter personvern opp mot de konkurrerende interessene sikkerhet og bekvemmelighet, viste derimot er tydelig sammenheng mellom graden av opptatthet av personvern og hvordan disse veies.

5.2 Personlige erfaringer og holdninger

I det følgende vil jeg undersøke den andre problemstillingen, *predikerer personlige negative erfaringer med tap av kontroll over personopplysninger et sterkere ønske om lovregulering av flyten av personopplysninger på nett*.

Som jeg har redegjort for i teorikapittelet baserer dagens internett seg i stor grad på en modell hvor innhold og tjenester tilbys gratis i bytte mot personopplysninger (Shapiro 1999, 160, Andrejevic 2014, 92-97, Papacharissi 2010a), noe som har muliggjort fremveksten av et lukrativt marked for personopplysninger (Hamelink 2000, 133, Shapiro 1999, 160). Dette markedet er preget av at individet, tilbyderen av personopplysninger, stiller svakt i møte med tjenestetilbyderne, og utbredt kunnskapsmangel blant brukerne er påvist i flere studier (for eksempel Turow 2003, Turow, Mulligan og Hoofnagle 2009, Smith 2014).

I tillegg er kontraktene, som fungerer som knutepunktet mellom de to partene, ofte preget av komplisert og tilslørende, juridisk språk (Sovern 1999, 1099, Jensen og Potts 2004, 477, Pollach 2007, 104). Videre er det ikke mulig å gjøre en meningsfull verdivurdering av informasjonen, siden den virkelige verdien først kan oppstå et sted langt frem i tid (Solove 2004, 87 – 88, Froomkin 2000, 1502 – 1503).

I tillegg er tilbaketrekning fra de samme plattformene for de færreste et reelt alternativ for de som er bekymret for eget personvern, noe som fører til at forbrukeren står ovenfor et dilemma med to ufordelaktige alternativer, enten å gi fra seg personopplysninger, eller lide et tap som følge av tilbaketrekning fra foraene (Lüders 2008, 104 – 105, Papacharissi 2010b, 47, Andrejevic 2009, 52).

Det er grunn til å hevde at disse egenskapene ved dagens internettmodell tvinger forbrukeren til å aksepterer en grad av registrering (Andrejevic 2014, 97, Marx 2006, 2). I lys av Nissenbaums teori om kontekstuell integritet (2010) er det imidlertid grunn til å anta at denne registreringen for de fleste ikke oppleves som særlig inngripende, og at mange vurderer sine egne personopplysninger som uinteressante i den enorme mengden informasjon som eksisterer digitalt (boyd 2007, 133).

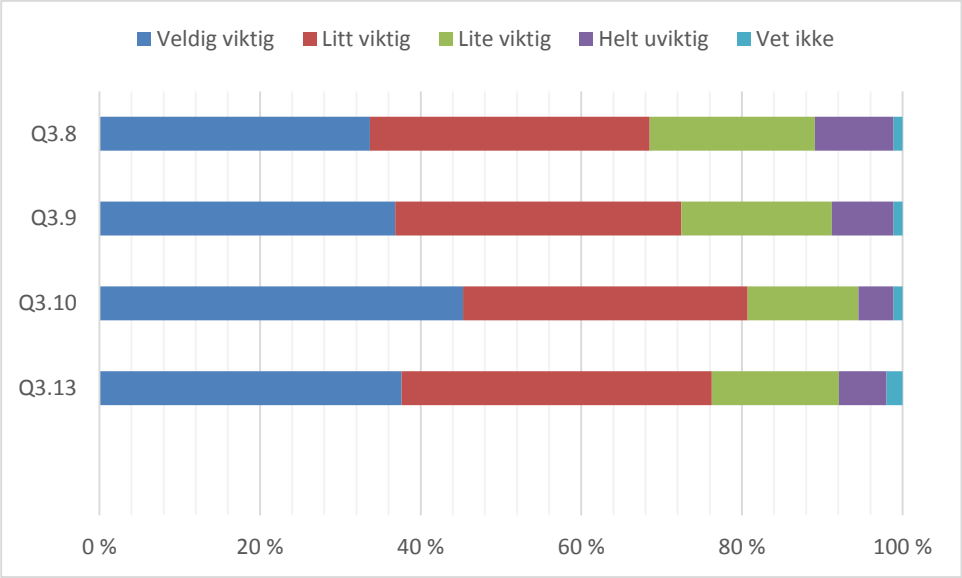
Jeg vil hevde at disse mekanismene i sum innebærer at byttehandelen internettbrukere inngår med innholds- og tjenestetilbydere på nett ikke kan kalles verken rettferdig eller meningsfull. Samtidig er det ingen tvil om at digital tilstedeværelse øker risikoen for å miste kontroll over

egne personopplysninger. Det er også et faktum at å leve i moderne informasjonssamfunn krever i det minste en grad av digital tilstedeværelse. Dermed er det nærliggende å tro at negative erfaringer vil prege holdninger om personvern i retning av mer restriktive holdninger, at man må brennes for å sky ilden. Jeg vil undersøke problemstillingen ved hjelp av regresjonsanalyser, med en konstruert, additiv indeks som avhengig variabel.

5.2.1 Avhengig variabel – en indeks

Det første steget blir dermed å opprette en indeks, noe jeg diskuterte i metodekapittelet. I dette kapittelet vil jeg gjennomføre en faktoranalyse for å finne «empiriske indikasjoner på om et indikatorsett representerer en tilfredsstillende operasjonalisering av et begrep» (Christophersen 2009, 205). Denne metoden bygger på indikatorenes kommunalitet, eller fellesvarians. Aller først vil jeg begynne med å presentere den univariate frekvensfordelingen på de enkelte variablene i figur 6.8:

Figur 6.8: Univariat frekvensfordeling av de fire variablene som vil inngå i den additive indeksen



Q3.8 – Opplysninger om steder du har vært og hvor du beveger deg, **Q3.9 –** Hvilke nettsteder du har besøkt/sett på, **Q3.10 –** Bilder av deg, **Q3.13 –** Hva du har søkt etter på søkemotorer.

Den univariate frekvensfordelingen er, som vi kan se, relativt lik på de fire variablene. Bilder av deg (Q3.10) vurderes som mest beskyttelsesverdig, mens opplysninger om steder du har vært og hvor du beveger deg (Q3.8) vurderes som minst beskyttelsesverdig. At bilder vurderes som mer beskyttelsesverdig enn digital informasjon vi etterlater oss som følge av

nettsidebesøk og bruk av søkemotorer er ikke overraskende, siden disse sannsynligvis vurderes som mer private enn nettaktivitet, slik jeg argumenterte for i metodekapittelet. Vi kan også observere at alternativene *veldig viktig* og *litt viktig* er overrepresentert, noe som viser et generelt stort ønske om lovregulering.

Faktoranalyse

I dette avsnittet vil jeg redegjøre for faktoranalysen og tilhørende reliabilitetstest. Fullstendige tabeller av analysen kan finnes som vedlegg 2. Variablene fremstår som umiddelbart relevante (face validity), som mål på ønske om lovmessig regulering. Det er likevel nødvendig å vurdere variablenes skjevhet og kurtose, fordi fordelingene bør være tilnærmet normalfordelte (Christophersen 2009, 205).

Tabell 6.1: Beskrivende statistikk for indikatorene

Holdning til lovregulering av flyten av personopplysninger på nett	N	Min	Max	Gj.snitt	Skjevhet (SE)		Kurtose (SE)	
Q 3.8	1484	,00	3,00	1,9346	-,521	,064	-,757	,127
Q 3.9	1484	,00	3,00	2,0270	-,628	,064	-,557	,127
Q 3.10	1484	,00	3,00	2,2298	-,892	,064	,030	,127
Q 3.13	1474	,00	3,00	2,1180	-,739	,064	-,208	,127
Valid N (listwise)	1463							

Tabell 6.1 viser at intervallet for kurtose og skjevhet er innenfor ± 1, noe som slår fast at avviket fra normalfordelingen ikke er et problem. Neste steg blir dermed gjennomføre en semi-konfirmerende endimensjonal faktoranalyse, med tanke på å opprette en additiv indeks.

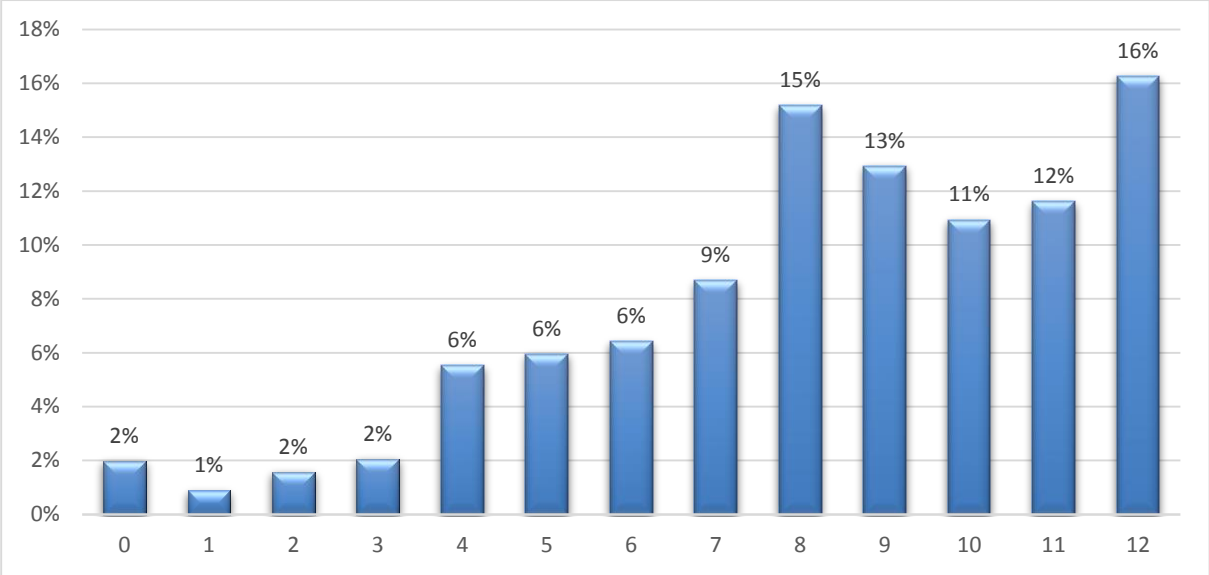
Denne analysen gir oss en Kaiser-Meyer-Olkin-verdi på 0,750, som indikerer at korrelasjonsmønsteret er tilfredsstillende for en faktoranalyse (KMO > 0,5) (Christophersen 2009, 207). I tillegg finner vi at Bartletts signifikanstest er 0, noe som slår fast at de bivariate indikator-korrelasjonene også er tilfredsstillende ($p < 0,05$) (Christophersen 2009, 210). I tillegg kan vi lese at faktor 1 har en eigenvalue på 2,636, noe som betyr at Kaisers kriterium (eigenvalue > 1) er oppfylt (Christophersen 2009, 211). Denne komponenten forklarer i tillegg hele 65 % av indikatorsettets varians.

Det siste steget i faktoranalysen er å gjennomføre en reliabilitetstest, for å måle indre konsistens, altså om indikatorsettet representerer en tilfredsstillende operasjonalisering av begrepet. Dette gjennomføres med Chronbachs alpha, som varierer mellom 0 og 1, der verdier

over 0,70 vurderes som tilfredsstillende for surveyundersøkelser (Christophersen 2009, 219). I vårt tilfelle måles denne til 0,826, noe som indikerer høy reliabilitet, og vi kan opprette indeksen.

Den opprettede indeksen har verdier som varierer fra 0 (respondenten har oppgitt 0 – helt uviktig – på samtlige spørsmål) til 12 (respondenten har oppgitt 3 – veldig viktig – på samtlige spørsmål). Samtlige enheter har dermed en indeksscore som representerer en addering av svarene hver enhet har avgitt på de fire spørsmålene som inngår i indeksen.

Figur 6.9: Frekvensfordeling, indeks



N=1463. Gjennomsnitt: 8,3. Median: 9

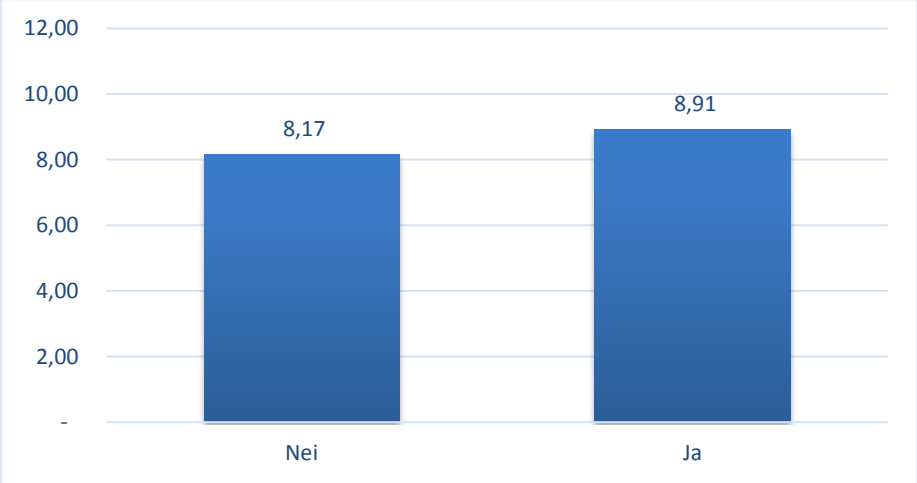
Som frekvensfordelingen presentert i figur 6.9 viser er det helt tydelig at lovregulering av salg og videre bruk av personinformasjon generert av vår digitale tilstedeværelse vurderes som viktig, slik også den univariate fordelingen i innledningen av avsnittet viste. Gjennomsnittet for indeksen er 8,3, altså så vidt over den gjennomsnittlige verdien for *litt viktig*. Den største gruppen finner vi helt til høyre i stolpediagrammet. Hele 16 prosent eller 238 av respondentene har valgt *veldig viktig* på samtlige variabler, noe som summert blir en faktorscore på 12.

5.2.2 Bivariate analyser – erfaringsvariablene

Som jeg har redegjort for ovenfor vil indeksen fungere som min avhengige variabel. Jeg vil i det følgende redegjøre for og diskutere variablene som vil inngå som uavhengige variabler. Jeg vil begynne med å presentere hvordan enhetene i de uavhengige variablene fordeler seg

med utgangspunkt i indeksens gjennomsnittsverdi. Dette gjør jeg for å grovt illustrere eventuelle sammenhenger hver for seg, før jeg lar alle inngå i samme modell til sist. Jeg vil først undersøke sammenhengen mellom de to variablene som omhandler tap av kontroll over personopplysninger på nett og den konstruerte indeksen. Disse er interessante da de i motsetning til de fleste av de andre spørsmålene fra undersøkelsen omhandler *erfaring*, og ikke holdninger. Dernest vil jeg gjøre det samme for de vanlige sosiodemografiske variablene alder, kjønn og utdanning. Den første erfaringsvariabelen jeg vil ta for meg er spørsmål 12 – *har du selv opplevd at personopplysninger om deg er kommet på avveie eller er blitt misbrukt av andre?*

Figur 6.10: Gjennomsnittsverdi på indeks fordelt på spørsmål 12 – *Har du selv opplevd at personopplysninger om deg er kommet på avveie eller er blitt misbrukt av andre?*



N=1282

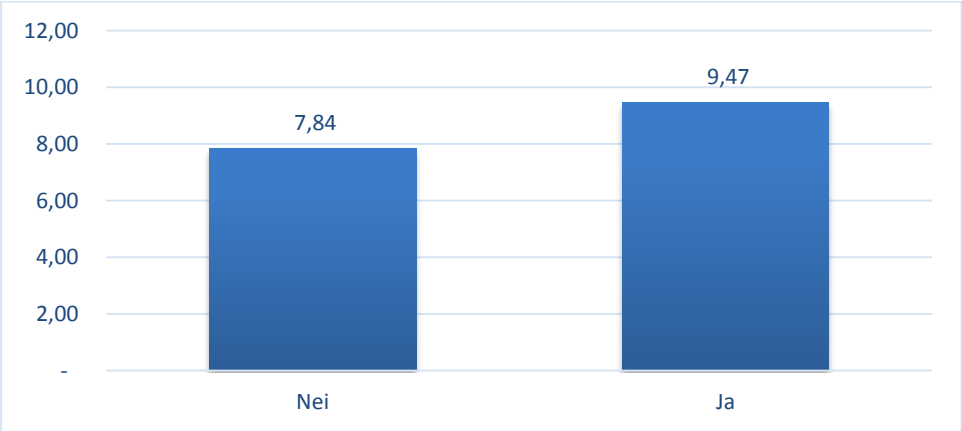
Figur 6.10 viser gjennomsnittsfordelingen på den konstruerte indeksen, gruppert etter svargivingen på spørsmål 12. Siden kategorien *vet ikke* også er fjernet fra denne variabelen blir antall respondenter justert ned. Å ha opplevd at personopplysninger kommer på avveie gjør, som vi kan lese av tabellen, at gjennomsnittet for holdning til lovregulering går noe opp. Det er imidlertid ikke snakk om noen enorm effekt. Det er i det hele tatt slående i hvor liten grad gjennomsnittet på den avhengige variabelen endres når denne første erfaringsvariabelen legges til grunn.

Den neste variabelen jeg vil ta for meg er spørsmål 13 – *har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skulle deles*. Jeg vil hevde at spørsmål 12 og 13 måler det samme, men at sistnevnte er en konkretisering av førstnevnte. Som jeg har diskutert i teorikapittelet er det grunn til å hevde at

kunnskapsmangel er en medvirkende årsak til at mange tilsynelatende ikke bryr seg nevneverdig om hvordan personopplysninger kjøpes og selges av tjenestetilbydere og nettselskaper (Turow 2003, 19, Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007). Når et spørsmål om tematikken er tilsvarende diffust kan det være de samme mekanismene som spiller inn i hvordan respondentene vurderer viktigheten av lovregulering. Derfor er det interessant å undersøke hvordan svarene fordeler seg når vi grupperer de etter den andre variabelen. Denne måler som nevnt det samme, men spørsmålet er av en mer konkret art.

Det er også verdt å merker seg at spørsmål 13 inkluderer forutsetningen «som du ikke ønsket skulle deles». Det kan hevdes at denne forskjellen kan påvirke respondentenes svargiving, og fra et personvernperspektiv kan man argumentere for at opplysningene det er snakk om faller inn under en annen konseptuell kategori enn spørsmål 12. Som jeg har forklart i teorikapittelet er nemlig *beskyttelse av sensitiv informasjon* en måte å forstå personverninteresser på som skiller seg fra en forståelse som ser personvern som *beskyttelse av all personbeskrivende informasjon* (Solove 2008, 22). Viktigheten av kontroll over personopplysninger vil avhenge av opplysningenes karakter og hvem som eventuelt har tilgang til informasjonen, det Nissenbaum kaller *korrekt informasjonsflyt* (2010, 2). Dermed vil ikke alle personopplysninger vurderes som like beskyttelsesverdige, selv om de fra et juridisk perspektiv er det.

Figur 6.11: Gjennomsnittsverdi på indeks fordelt på spørsmål 13 – *Har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skulle deles?*



N=1370

Figur 6.11 viser gjennomsnittet på indeksen gruppert etter spørsmålet som omhandler *uønsket bildepublisering*. Sammenligner vi funnene fra de to spørsmålene kan vi tydelig se at uønsket

bildepublisering i større grad gir utslag på gjennomsnittet på indeksen. Dette er en interessant observasjon i lys av Nissenbaums teori om *kontekstuell integritet* (2010). Det er grunn til å tro at de som har opplevd uønsket bildepublisering i større grad opplever det som et brudd på sin kontekstuelle integritet, enn det mer diffuse spørsmålet om personopplysninger på avveie. Uønsket bildepublisering og misbruk av private bilder er også med jevne mellomrom gjenstand for medieoppmerksomhet (Blaker 2011).

Det er altså grunn til å hevde at spørsmål 13 representerer en konkretisering av spørsmål 12. Det er også sannsynlig at respondentene tolker begrepet *personopplysninger* som mer trivielle enn bilder, som ofte kan være svært private. I tillegg kan det hende at å ferdes på nett oppleves som en digital parallell til å ferdes i det offentlige rom for øvrig, noe som innebærer en større aksept for registrering enn hva tilfelle er innenfor husets fire vegger. På samme vis er bilder noe som i utgangspunktet hører hjemme i privatsfæren, og at bilder i økende grad eksisterer digitalt innebærer at det private flyttes vekk fra denne sfæren og over i en sfære med mindre grad av kontroll.

5.2.3 Bivariate analyser – kontrollvariablene alder, kjønn og utdanning

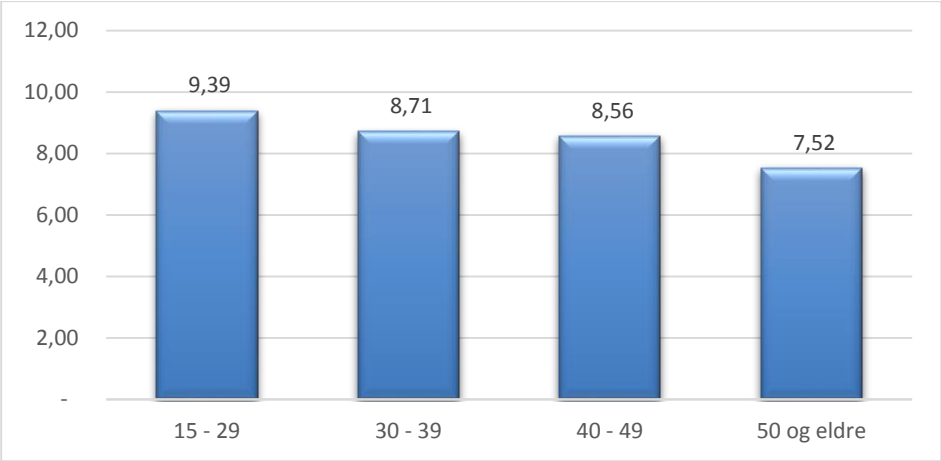
Etter å ha presentert fordelingen på de to erfaringsvariablene vil jeg nå ta for meg kontrollvariablene som vil inngå i regresjonsanalysen. Jeg har valgt å inkludere variablene *alder*, *kjønn* og *utdanning*. Variabelen *inntekt* velger jeg å ikke kontrollere for, da et for stort antall respondenter har valgt å ikke oppgi dette (39,4 prosent).

Alder

Det er grunn til å tro at alder har stor innvirkning på hvordan vi vurderer viktigheten av juridisk beskyttelse av personopplysninger. Unge mennesker har jevnt over en større digital tilstedeværelse enn eldre, noe som kan hevdes å sannsynliggjøre et sterkere ønske om lovregulering. I tillegg er det grunn til å tro at yngre mennesker har mer kunnskap om internett, og følgelig implikasjonene av å ta i bruk digitale tjenester og verktøy. En undersøkelse fra 2013 viste at yngre mennesker i større grad enn eldre tar grep for å bli mindre synlige på nett (Rainie et al. 2013, 10). Samtidig kan nettopp det at den yngre generasjonen har «vokst opp digitalt» være en grunn til at de ikke ser på lovregulering som nødvendig. Facebook-sjef Mark Zuckerberg har for eksempel hevdet at personvernnormer i

befolkningen endres, og at «folk er mer komfortable med å dele mer informasjon med flere mennesker» (Kirkpatrick 2010). Zuckerberg refererer ikke til noen aldersgruppe, men majoriteten av Facebook-brukere er unge mennesker.

Figur 6.12: Gjennomsnittsverdi på indeksen fordelt på *alder*



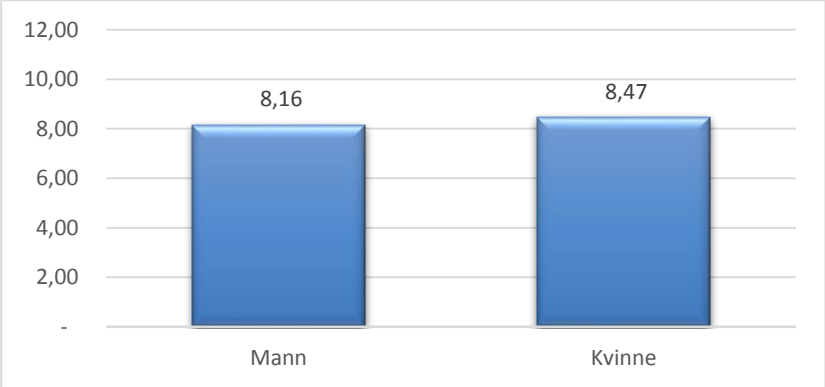
N=1463

Figur 6.12 viser at ønsket om lovregulering er klart størst i den yngste aldersgruppen. Den eldre garde, de over 50, skiller seg ut som minst opptatt av lovregulering av våre digitale fotavtrykk. Tallene kan altså sies å bekrefte den første antakelsen over. Yngre mennesker vurderer lovregulering av digitale fotavtrykk som viktigere enn eldre.

Kjønn

Det er i utgangspunktet liten grunn til å tro at kjønn vil påvirke ønske om lovregulering i særlig grad.

Figur 6.13: Gjennomsnittsverdi på indeksen fordelt på *kjønn*



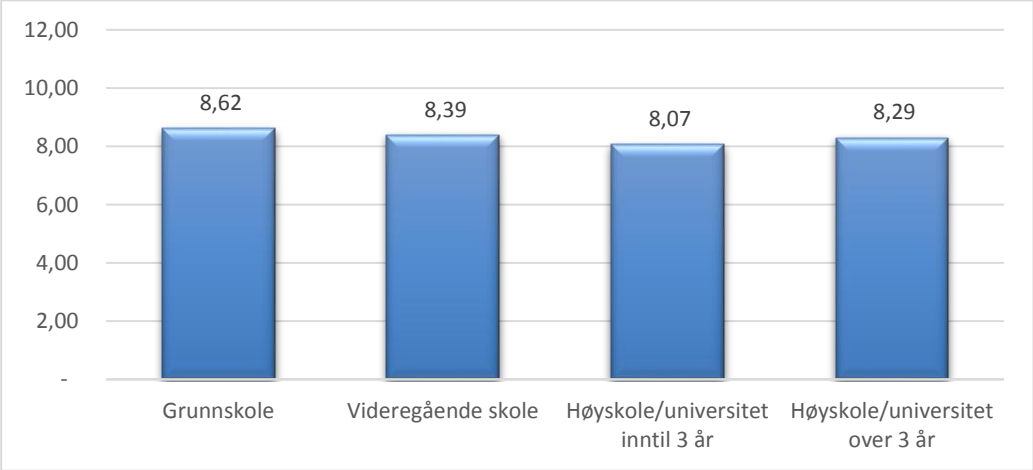
N=1463

Figur 6.13 viser altså at menn i noe mindre grad enn kvinner mener det er viktig at lovverket beskytter informasjonsflyten på nett. Det er imidlertid ikke snakk om noe stor forskjell.

Utdanning

Utdanning vil være den siste sosiodemografiske variabelen jeg undersøker. Som jeg har drøftet i teorikapittelet, er en medvirkende årsak til at mange handler i strid med egne personvernholdninger at implikasjonene av handlingene ikke forstås. I tillegg har undersøkelser vist at mange tjenesteavtaler som eksisterer på internett er skrevet på et språk som forutsetter mange års skolegang for å forstå (for eksempel Pollach 2007, 104). Det er dermed nærliggende å tro at høy utdannelse øker sannsynligheten for kunnskap om informasjonsflyten på nett, og dermed et ønske om lovregulering.

Figur 6.14: Gjennomsnittsverdi på indeksen fordelt på *utdanning*



N=1430

Som figur 6.14 viser holder ikke antakelsen om at høy utdanning øker ønsket om lovregulering vann. Funnene presentert i figur 6.14 må sies å være svært overraskende. Svarfordelingen er veldig jevn, men den laveste utdanningsgruppen oppnår den høyeste verdien på gjennomsnittet av indeksen.

Det kan hevdes at nettopp det at tjenesteavtalene, møtepunktet mellom tjenestetilbydere og brukere, ofte er formulert på vanskelig, tungt juridisk språk fører til at mennesker uten høy utdannelse gir opp å handle som selvstendig kunde på markedet, og dermed er mer tilbøyelige til å se mot myndighetene for beskyttelse enn de med høy utdannelse. Et slikt syn er særlig interessant på bakgrunn av undersøkelsene som viste at personvernerklæringer på internett er

skrevet på et språk som krever leseferdigheter over det antatte gjennomsnittet av internettbrukere i USA (Pollach 2007).

Det er imidlertid en høyst tvilsom antakelse at mennesker med høy utdannelse leser gjennom og fullstendig forstår samtlige tjenesteavtaler de godtar på nett, samt implikasjonene av surfing og bruk av søkemotorer fra et personvernperspektiv. Det er uansett en interessant observasjon at utdanning ikke påvirker ønsket om lovregulering av flyten av personopplysninger på nett.

5.2.4 Bivariate regresjonsanalyser - erfaringsvariablene

Siden problemstillingen jeg ønsker å undersøke omhandler personlige negative erfaringer med tap av kontroll over personopplysninger vil jeg i modell 1 og 2 (tabell 6.3) undersøke de to variablene som omhandler dette, hver for seg i lineære, bivariate regresjoner. Dette gjør jeg for å kartlegge den selvstendige effekten de to variablene har på den avhengige variabelen. I modell 3 (tabell 6.4) inngår de samme variablene i en simultan regresjonsanalyse. I modell 4, 5 og 6 (tabell 6.4) vil jeg inkludere de sosiodemografiske kontrollvariablene i en sekvensiell, multivariat regresjonsanalyse, for å kontrollere effekten av disse på den avhengige variabelen, og også kontrollere om effekten av de to erfaringsvariablene endrer seg når samtlige variabler inngår.

I modell 1 vil jeg undersøke variabelen *har du selv opplevd at personopplysninger om deg er kommet på avveie, eller er blitt misbrukt av andre* (Q 12). I modell 2 vil jeg undersøke den andre erfaringsvariabelen, *har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skille deles* (Q 13).

Tabell 6.3: Lineær, bivariat regresjonsanalyse med indeksen som avhengig variabel og henholdsvis Q12 (modell 1) og Q13 (modell 2) som uavhengige variabler.

Uavhengige variabler	**Modell 1**			**Modell 2**		
	b	SE(b)	Beta	b	SE(b)	Beta
Konstant	8,908	0,258		7,836	0,090	
Q 12	0,742**	0,272	0,076	-	-	-
Q 13	-	-	-	1,631***	0,176	0,243
Justert R^2	**0,006**			**0,059**		

**p<0,05, **p<0,01, ***p<0,001, N= 1282*

Q12: Har du selv opplevd at personopplysninger om deg er kommet på avveie, eller er blitt misbrukt av andre?

Q13: Har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skille deles

Tabell 6.3 viser resultatene av de bivariate regresjonsanalysene med indeksen som avhengig variabel og henholdsvis spørsmål 12 (modell 1) og spørsmål 13 (modell 2) som uavhengige variabler.

Modell 1 viser at når verdien på skalaen til spørsmål 12 går opp ett nivå – altså fra *nei, jeg har ikke opplevd* til *ja, jeg har opplevd*, øker verdien på indeksen med 0,742. Bidraget er signifikant på et 1 % nivå, noe som betyr at sammenhengen mellom erfart mangel på kontroll og holdning til lovregulering ikke er tilfeldig (Hjerm og Lindgren 2011, 82). Justert R^2 indikerer statistisk forklart variasjon, altså modellens forklaringskraft (Hjerm og Lindgren 2011, 76). Denne er i modell 1 på 0,006, altså forklarer modellen 0.6 % av variasjonen i den avhengige variabelen, noe som innebærer at modellen har en svært svak forklaringskraft. Dette er i utgangspunktet ikke overraskende, tatt i betraktning de små utslagene denne variabelen hadde i den bivariate analysen ovenfor.

I modell 2 har jeg undersøkt effekten av den andre erfaringsvariabelen, som omhandler *uønsket bildepublisering*. Denne variabelen vil jeg som nevnt hevde kan leses som en konkretisering av den forrige, ved å spørre eksplisitt om bilder. Modell 2 viser at når denne variabelen øker med ett nivå, fra *nei, jeg har ikke opplevd* til *ja, jeg har opplevd*, øker verdien på indeksen med 1,631. Variabelen som omhandler uønsket bildepublisering har altså en mye sterkere påvirkningskraft på den avhengige variabelen enn variabelen som spør om *personopplysninger på avveie.* Dette bidraget er i tillegg klart signifikant. I tillegg kan vi observere at juster R^2 i denne modellen måles til 0,059. Dette innebærer følgelig at modell 2

forklarer en mye større del av variasjonen på den avhengige variabelen enn modell 1. 0,059 tilsvarer 5,9%, så modell 2 har heller ikke en stor forklaringskraft.

5.2.5 Multivariate regresjonsanalyser

I den neste tabellen vil jeg som nevnt inkludere de sosiodemografiske variablene *alder*, *kjønn* og *utdanning*, i tillegg til de to erfaringsvariablene, i en multivariat regresjonsanalyse. Hver uavhengige variabel inkluderes sekvensielt. Modell 3 inneholder således de to erfaringsvariablene. Modell 4 inkluderer *alder*, modell 5 inkluderer *kjønn* og endelig inkluderer modell 6 den siste kontrollvariabelen, *utdanning.* Å inkludere variablene trinnvis på denne måten tydeliggjør hvilken effekt hver uavhengige variabel har, i tillegg til at eventuelle endringer på de andre variablene kan observeres fortløpende.

Tabell 6.4: Sekvensiell regresjonsanalyse med indeksen som avhengig variabel og Q12, Q13 samt alder, kjønn og utdanning som uavhengige variabler

	Modell 3			**Modell 4**			**Modell 5**			**Modell 6**		
Uavhengige variabler	B	SE(b)	Beta	B	SE(b)	Beta	B	SE(b)	Beta	B	SE(b)	Beta
Konstant	7,759	0,098		8,696	0,243		8,608	0,197		8,486	0,243	
Q12	0,290	0,282	0,029	0,322	0,278	0,032	0,318	0,278	0,032	0,310	0,278	0,031
Q13	1,639***	0,194	0,239	1,130***	0,209	0,165	1,115***	0,210	0,163	1,111***	0,210	0,162
Alder	-	-	-	-0,447***	0,074	-0,181	-0,449***	0,074	0,182	-0,460***	0,075	-0,187
Kjønn	-	-	-	-	-	-	0,193	0,164	0,032	0,193	0,164	0,033
Utdanning	-	-	-	-	-	-	-	-	-	0,075	0,087	0,024
Justert R^2	0,059			0,086			0,086			0,086		

**p<0,05, **p<0,01, ***p<0,001, N=1210*

Modell 3 viser effekten av spørsmål 12, kontrollert for spørsmål 13, på den avhengige variabelen, som altså er den opprettede indeksen som måler *holdning til lovregulering av flyten av personopplysninger på nett*. Modellen viser at effekten spørsmål 12 har på den avhengige variabelen synker merkbart, fra 0,742 til 0,290. Dette betyr at mye av effekten Q12 hadde på den avhengige variabelen vist i modell 1, kan tilskrives den andre erfaringsvariabelen, altså Q13.

Spørsmålet om uønsket bildepublisering (Q13) har en mye høyere påvirkningskraft på den avhengige variabelen. Når denne variabelen går opp ett nivå, fra *nei, jeg har ikke opplevd* til *ja, jeg har opplevd*, øker verdien på indeksen med 1,639. Dette bidraget er i tillegg klart signifikant. Det er også verdt å merke seg at Q12 mister sin signifikans når vi kontrollerer for Q13. Dette innebærer at mye av påvirkningskraften vist i modell 1 blir borte når vi kontrollerer for Q13. Justert R^2 er i tillegg lik i modell 3 som i modell 2, altså den bivariate regresjonsanalysen med *uønsket bildepublisering* (Q13) som uavhengig variabel, noe som antyder at denne variabelen forklarer nesten all variasjonen i den avhengige indeksvariabelen. Det er viktig å påpeke at påvirkningen på de to erfaringsvariablene er noe endret fra modell 1 og 2 som inkluderer de samme variablene i bivariate regresjoner, siden modellen ekskluderer enhetene som ikke har oppgitt *utdanning*.

I modell 4 undersøkes effekten av de to erfaringsvariablene, kontrollert for den uavhengige variabelen *alder*. Av tabellen kan vi lese at når aldersvariabelen øker med ett nivå *synker* verdien på den avhengige indeksvariabelen med 0,447. Siden aldersvariabelen går fra lav til høy alder innebærer dette at når aldersvariabelen øker fra for eksempel 0 (15 – 29 år) til 1 (30 – 39 år) går holdningen til lovregulering av flyten av personopplysninger på nett *ned* med 0,477. Lovregulering vurderes altså som mindre viktig jo eldre man blir, noe de bivariate analysene også antydet. Dette bidraget er i tillegg klart signifikant. Justert R^2 øker i tillegg, fra 0,059 i modell 3 til 0,086 i modell 4. Dermed kan vi slå fast at effekten de to erfaringsvariablene, kontrollert for alder øker modellens forklaringskraft. Fremdeles forklarer ikke modellen en stor del av variasjonen på den avhengige variabelen, men økningen er relativt sett stor. Variabelen som omhandler *uønsket bildepublisering*, som i modell 3 viste seg å ha stor innvirkning på i den avhengige variabelen, mister noe av sin påvirkningskraft når vi kontrollerer for *alder* i modell 4. Bidraget er imidlertid fremdeles klart signifikant. Dette er sannsynligvis forbundet med at unge mennesker i større grad enn eldre har en høy digital tilstedeværelse og er mer vant til å publisere bilder på nett. Undersøkelsen *Anonymity, Privacy and Security Online* fant at ung alder øker sannsynligheten for at det finnes personinformasjon på nett, inkludert bilder (Rainie et al. 2013, 14). Dermed øker også sannsynligheten for uønsket bildepublisering. Det er imidlertid viktig å understreke at begge variablene har en selvstendig effekt, selv om effekten av *uønsket bildepublisering* gikk noe ned kontrollert for *alder*. Dette innebærer at variabelen *uønsket bildepublisering* ikke fanger opp hele spekteret av erfaringer som kan predikere et sterkere ønske om lovregulering. Dette

fremstår som rimelig, all den tid uønsket bildepublisering åpenbart ikke er den eneste erfaringen som kan predikere en slik holdningsendring.

Modell 5 inneholder de *to erfaringsvariablene* og *alder*, kontrollert for *kjønn.* Av tabellen kan vi lese at når denne øker ett nivå, fra *mann* til *kvinne,* øker verdien på den avhengige variabelen med 0,193. Bidraget er ikke signifikant, og endrer heller ikke modellens forklaringskraft, justert R^2. De andre variablenes påvirkning på den avhengige variabelen endrer seg marginalt, noe som antyder at variabelen kjønn har svært liten påvirkning.

Modell 6 inkluderer de to *erfaringsvariablene, alder* og *kjønn,* kontrollert for *utdanning*. Når verdien på denne variabelen øker med ett nivå, øker verdien på den avhengige variabelen med 0,075. Bidraget er ikke signifikant. Effekten de andre variablene har endrer seg i tillegg svært lite, og justert R^2, altså modellens forklaringskraft endres heller ikke. Denne variabelens manglende påvirkning på den avhengige variabelen er et interessant funn, på bakgrunn av at *kunnskapsmangel* er et av de største problemene med dagens internettmodell (Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007, Turow 2003, 19). Det hadde vært nærliggende å tro at høy utdannelse innebærer mer kunnskap om hvordan personinformasjon kjøpes og selges på et marked, og følgelig predikert et sterkere ønske om lovregulering. Variabelen utdanning har imidlertid ingen påvirkningskraft, og de andre variablenes effekt endres heller ikke.

5.2.6 Oppsummering

Denne siste analysedelen har vist at personlige erfaringer med *uønsket bildepublisering* predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett. Når spørsmålet derimot omhandler det mer diffuse begrepet *personopplysninger på avveie* er denne effekten mye mindre. I tillegg predikerer *lav alder* et sterkere ønske om lovregulering, samtidig som effekten av variabelen *uønsket bildepublisering* synker noe, kontrollert for *alder*. Det er nærliggende å tro at dette kommer av at yngre mennesker er mer sårbare for slike hendelser på grunn av større digital tilstedeværelse. Kjønn og utdanning ikke har noen merkbar effekt.

Uønsket bildepublisering og *lav alder* predikerer altså et sterkere ønske om lovregulering av flyten av personopplysninger på nett. Det er imidlertid viktig å fremheve at ønsket om lovregulering av flyten av personopplysninger på nett i utgangspunktet er sterkt på tvers av

aldersgruppene. Dette er i tråd med Fox' undersøkelse som viste at en overveldende majoritet – 86 prosent – ønsker en endring i dagens praksis, konkretisert gjennom at selskapene må spørre om lov for å samle inn informasjon på forhånd (Fox et al. 2000, 2).

6 Diskusjon og oppsummering

Digital tilstedeværelse genererer digitalt gull, og markedet der personopplysninger byttes mot innhold og tjenester på nett har en rekke problematiske egenskaper fra et personvernperspektiv. Disse setter nettbrukerne i en posisjon uten reell forhandlingsmakt, og tvinger oss alle til å bidra til den storstilte, informasjonsbaserte verdiskapingen.

Mine analyser har vist at det *ikke* er en sammenheng mellom graden av opptatthet av personvern og villighet til å ta i bruk personvernkrenkende teknologi. På et overgripende, normativt nivå har jeg vist at graden av opptatthet av personvern *har* sammenheng med hvordan personvernet veies opp mot de konkurrerende interessene *sikkerhet* og *bekvemmelighet*. Disse to funnene sett i sammenheng indikerer at personvern veies ulikt på et *individuelt* nivå i forhold til et *generelt* nivå.

Videre har jeg påvist at *personlige negative erfaringer med uønsket bildepublisering* og *lav alder* predikerer et sterkere ønske om lovregulering av flyten av personopplysninger på nett. *Utdanning* har derimot ingen påvirkningskraft på ønsket om lovregulering, slik man kanskje ville anta. I tillegg vil jeg hevde at en viktig observasjon kan identifiseres allerede i starten av analysen: det generelle ønsket om lovregulering av flyten av personopplysninger på nett er sterkt. Dette er viktig å huske på når jeg etterpå drøfter hvordan de ulike variablene påvirker ønsket om lovregulering.

På bakgrunn av analysene som jeg har presentert i forrige kapittel vil jeg i dette kapittelet tolke og diskutere funnene opp mot teoretiske perspektiv, metodiske valg og utfordringer og tidligere undersøkelser. Jeg vil dele denne delen i to, hvor del 6.1 tar for seg den første problemstillingen og del 6.2 tar for seg den andre. De to problemstillingene er imidlertid ikke fullstendig løsrevet fra hverandre, og flere av de teoretiske perspektivene vil være relevante for begge problemstillinger.

6.1 Sammenheng mellom ulike holdninger

I dette kapittelet vil jeg oppsummere og diskutere funnene fra analysedelen som skulle undersøke den første problemstillingen, *finnes det en sammenheng mellom hvor opptatt man er av personvern* og (a) *hvor villig man er til å ta i bruk personvernkrenkende teknologi* og (b) *hvordan man veier personvernet opp mot andre interesser på et overordnet nivå.*

Hvor opptatt man er av personvern har ingen sammenheng med hvor villig man er til å ta i bruk personvernkrenkende teknologi

Den første delen av den første problemstillingen tok sikte på å undersøke om det finnes en sammenheng mellom *hvor opptatt man er av personvern og hvor villig man er til å ta i bruk personvernkrenkende teknologi.* Problemstillingen søker altså å kartlegge en sammenheng mellom en overgripende normativ holdning og en tenkt handling, som dermed også må tolkes som et holdningsspørsmål.

Det mest slående funnet i den første analysen er den nærmest totale mangelen på sammenheng mellom de to holdningsvariablene. De som oppgir å være *svært opptatt av personvern* er like villige til å GPS-spore egne barn som de som oppgir å være *lite opptatt av personvern* (figur 6.3). Det er faktisk flere av de som er *svært opptatt av personvern* som kan tenke seg å benytte Google-briller, enn blant de som er *lite opptatt av personvern* (figur 6.4).

I spørsmålet om villighet til å ta i bruk teknologi som legger press på personvernet ligger det implisitt en interesseavveiing. Dette er fordi teknologien det spørres om åpenbart utfyller ønskelige funksjoner, og de personverntruende egenskapene kan tolkes som å være en bieffekt av disse. Slike interesseavveiinger er en uunngåelig konsekvens av å leve i et pluralistisk, moderne samfunn (Nissenbaum 2010, 110, Schartum og Bygrave 2011, 43). Hvordan disse interesseavveiingen vurderes – og om de vurderes overhode – gir ikke spørsmålet anledning til å besvare. Det er likevel overveiende sannsynlig at interessene veies opp mot hverandre, all den tid spørsmålet inngår i en undersøkelse om personvern.

Det kan videre argumenteres for at interesseavveiingen er mer åpenbar i spørsmålet om GPS-sporing av egne barn enn spørsmålet om Google-briller. Sistnevnte teknologi er ennå ikke lansert på det norske markedet, og har ikke selvforklarende egenskaper, slik GPS-sporing av egne barn har. I tillegg kan man hevde at de personvernkrenkende egenskapene ved Google-briller kan kontrolleres – at det er mulig å ta i bruk brillene uten at det går på akkord med personvernprinsipper. De personverntruende egenskapene ved GPS-sporing av egne barn er på den annen side de samme egenskapene som gjør teknologien tiltrekkende. Det vil ikke gå an å GPS-spore barn uten at det går på akkord med personvernprinsipper, mens Google-briller kan brukes ansvarlig.

Å bruke eller ikke bruke disse to ulike teknologiene representerer også to ulike interesseavveiinger. Det er med andre ord ikke samme interesse som settes opp mot

personvernet når man vurderer å ta i bruk GPS-sporing av egne barn og Google-briller. Førstnevnte teknologi representerer en uhyre effektiv måte å sørge for at du til enhver tid vet hvor barnet ditt befinner deg, og følgelig at det er trygt, eller i det minste at du raskt kan komme til unnsetning i en krisesituasjon. Dermed vil en vurdering av denne teknologien representere en interesseavveiing mellom *personvern* og *sikkerhet*.

Google-briller på den annen side er et eksempel på teknologi som gjør daglige gjøremål og oppgaver mer *bekvemmelige* og *effektive*. I tillegg er det sannsynlig at å ta i bruk den aller siste nyvinningen fra Silicon Valley for mange signaliserer status. Det er dermed sannsynlig at selv om personvernholdninger tilsynelatende ikke har en sammenheng med hvor villig man er til å ta i bruk personverntruende teknologi, er det høyst ulike interesseavveiinger som ligger til grunn for de to eksemplene.

Hvor opptatt man er av personvern *har* sammenheng med hvordan man veier personvernet opp mot andre interesser på et overordnet nivå

Andre del av den første problemstillingen tok sikte på å undersøke om det finnes en sammenheng mellom *hvor opptatt man er av personvern og hvordan man veier personvernet opp mot andre interesser på et overordnet nivå.*

Den første analysedelen viste altså at det ikke kan påvises en sammenheng mellom overordnede holdninger til personvern og villighet til å ta i bruk teknologi som legger press på personvernet. I tillegg argumenterte jeg for at et viktig, implisitt premiss for spørsmålet om ny teknologi er den interesseavveiingen som gjøres. De neste analysene viste at graden av opptatthet av personvern *har* sammenheng med hvordan personvernet vurderes opp mot de konkurrerende interessene *sikkerhet* og *bekvemmelighet*, når disse avveiingene vurderes *på et overordnet nivå.* I disse krysstabellanalysene valgte jeg å gjøre om svarene til dikotome variabler, for å tydeliggjøre svarfordelingen. *Helt enig* og *delvis enig* på den ene siden og *helt uenig* og *delvis uenig* på den andre.

Den første interesseavveiingen jeg tok for meg setter personvern opp mot *sikkerhet.* Igjen er det viktig å minne om at dette er en uunngåelig og nødvendig interesseavveiing, hvor personvernet på ingen måte er enerådende (Schartum og Bygrave 2011, 44). Analysen viste at hvor opptatt man er av personvern *har* sammenheng med hvor enig man er i påstanden *vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet* (figur 6.6). Omtrent dobbelt

så mange av de som oppgir å være *lite opptatt* av personvern sier seg helt eller delvis enige i påstanden som de som er *svært opptatt* av personvern. Med andre ord viser funnene en tydelig tendens til at hvor opptatt man er av personvern har sammenheng med hvordan man veier personvernet opp mot den konkurrerende interessen *sikkerhet* på et overordnet nivå.

Den samme tendensen ble påvist i analysen som undersøkte sammenhengen mellom graden av opptatthet av personvern og påstanden *offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulige effektive tjenester* (figur 6.7). Dette er en interesseavveiing som setter personvernet opp mot interessen som jeg har klassifisert som *bekvemmelighet.* I dette eksempelet relaterer bekvemmelighet til mer effektiv tjenesteformidling fra det offentlige.

Igjen kan vi se en tydelig sammenheng mellom hvor opptatt man er av personvern og hvordan man veier personvernet opp mot denne interessen. Omtrent halvparten av de som er *svært opptatt* av personvern motsetter seg slik informasjonsdeling, mot litt over en fjerdedel av de som er *lite opptatt* av personvern. På samme måte som når sikkerhet veies opp mot personvern viser denne analysen at hvor opptatt man er av personvern har sammenheng med hvordan man veier dette opp mot den konkurrerende interessen *bekvemmelighet*, på et overordnet nivå.

Individuelle og generelle interesseavveiinger vurderes ulikt

De to siste krysstabellanalysene viser altså at graden av opptatthet av personvern *har* sammenheng med hvordan man veier personvernet opp mot andre interesser på et overordnet nivå (figur 6.6 og 6.7). Krysstabellanalysene som sammenlignet graden av opptatthet av personvern med villighet til å ta i bruk personverntruende teknologi viste derimot ingen slik sammenheng, selv om også å ta i bruk slik teknologi representerer en lignende interesseavveiing (figur 6.3 og 6.4).

Det er nærliggende å tro at nettopp det at spørsmålene i den andre analysedelen eksplisitt artikulerer interessemotsetningene øker sannsynligheten for disse blir grundig vurdert. I tillegg kan det tenkes at påstandenes overgripende, normative karakter gjør at respondentene vurderer de som viktigere enn hva tilfelle er med valg om å benytte teknologi på privat basis.

Jeg har argumentert for at de to spørsmålene om villighet til å ta i bruk teknologi representerer en interesseavveiing, i likhet med de overgripende spørsmålene som eksplisitt artikulerer

disse avveiingene. Like fullt er det først når disse avveiingen løftes opp på et overgripende nivå at graden av opptatthet av personvern har sammenheng med hvordan de veies.

Schartum og Bygrave (2011, 43) skiller i sin redegjørelse av interesseteorien mellom *individuelle* og *generelle* interesseavveiinger. Individuelle interesseavveiinger betegner «de situasjoner der den enkelte person selv tar stilling til hvor stor vekt han eller hun vil tillegge personvernhensyn i forhold til private hensyn». Generelle interesseavveiinger på den annen side forklares som:

> De allmenne vurderinger som politiske myndigheter, tilsynsmyndigheter, behandlingsansvarlige og andre må gjennomføre av forholdet mellom personvernmessige, økonomiske og andre konsekvenser av et generelt opplegg for behandling av personopplysninger (Schartum og Bygrave 2011, 43).

Mine funn antyder at personvernet tillegges større betydning i de *generelle* interesseavveiingene enn i de *individuelle*. Dette kan tolkes som at personvernholdninger har betydning i en overordnet debatt om samfunnsutviklingen. Det kan også hevdes at et slikt funn anerkjenner makten som ligger i å ha enorme dataregistre om store deler av befolkningen, slik offentlige myndigheter har. Frykten for hvilken makt som ligger i tilgangen til slike registre har vært drivkraften bak personvernteori som skiller ut *personopplysningsvern* som en egen kategori på feltet (Westin 1967, 158, Solove 2008, 24, Selmer og Blekeli 1977, 16).

På den annen side er det et åpenbart paradoks at ikke sterke personvernholdninger gjenspeiles i de *individuelle* interesseavveiingene. Det hadde i utgangspunktet vært nærliggende å tro at overordnede personvernholdninger i større grad ble gjenspeilet i individuelle avveiinger med hensyn til personvern. Mine funn antyder at imidlertid at dette ikke er tilfelle.

6.2 Personlige erfaringer og holdninger

I den andre analysedelen ville jeg undersøke om *personlige negative erfaringer med tap av kontroll over personopplysninger predikerte et sterkere ønske om lovregulering av flyten av personopplysninger på nett.* Jeg opprettet en additiv indeks og benyttet denne som avhengig variabel. Som uavhengige variabler valgte jeg ut to *erfaringsvariabler,* samt de sosiodemografiske variablene *alder*, *kjønn* og *utdanning*. De innledende, bivariate analysene viste at erfaringsvariabelen som omhandlet *uønsket bildepublisering* hadde en effekt på

gjennomsnittet på den avhengige variabelen (figur 6.11). I tillegg predikerte *lav alder* et sterkere ønske om lovregulering (figur 6.12).

Videre gjennomførte jeg først to bivariate, lineære regresjoner med de to erfaringsvariablene som uavhengig variabel (tabell 6.3). Disse bekreftet at *uønsket bildepublisering* hadde relativt stor påvirkningskraft på indeksen. Så gjennomførte jeg en sekvensiell regresjonsanalyse, hvor samtlige variabler ble inkludert trinnvis (tabell 6.4). I tillegg til effekten variabelen med *uønsket bildepublisering* hadde, predikerte *lav alder* et høyere ønske om lovregulering, slik de bivariate analysene antydet.

Uønsket bildepublisering og lav alder predikerer et sterkere ønske om lovregulering

At mennesker som har opplevd *uønsket bildepublisering* ønsker et sterkere juridisk vern for flyten av personopplysninger på nett er ikke overraskende. I tillegg til denne erfaringsvariabelen viste regresjonsanalysen at *lav alder* på samme måte predikerte et sterkere ønske om lovregulering. Disse to observasjonene må sees i sammenheng, da yngre mennesker oftere har bilder, og annen personinformasjon, liggende på nett (Rainie et al. 2013, 14). Samme undersøkelse viste også at yngre mennesker i større grad tar grep for å sikre egen anonymitet på nett (Rainie et al. 2013, 10). Det er på samme vis sannsynlig at denne tematikken – uønsket bildepublisering – for mange over 50 år er helt ukjent.

Samtidig viser analysene at begge variablene har en selvstendig effekt på indeksvariabelen, selv om effekten av *uønsket bildepublisering* gikk noe ned kontrollert for *alder*. Dette antyder at erfaringsvariablene jeg har benyttet i analysene ikke tegner et fullstendig bilde av hvilke erfaringer som preger ønsket om lovregulering, noe som fremstår som logisk. Uønsket bildepublisering er åpenbart ikke den eneste erfaringen som kan predikere et sterkere ønske om lovregulering.

Den andre erfaringsvariabelen som jeg undersøkte, *har du selv opplevd at personopplysninger om deg er kommet på avveie, eller er blitt misbrukt av andre*, hadde på den annen side liten påvirkningskraft på ønsket om lovregulering av flyten av personinformasjon på nett (tabell 6.3). Det er grunn til å tro at formuleringen av dette spørsmålet kan ha hatt betydning for et slikt resultat. Begrepet *personopplysninger* omfatter i prinsippet mye informasjon som mange ikke nødvendigvis vurderer som beskyttelsesverdige. Hvis man forstår personvern som «en

mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem» (Selmer og Blekeli 1977, 13), vil alle opplysninger som høstes fra vår digitale tilstedeværelse rammes av definisjonen. Det er likevel ikke sikkert alle mennesker legger denne brede forståelsen av personvern til grunn når de vurderer spørsmålet, og denne begrepstolkningen vil påvirke svargivingen. Det kan hende at begrepet *personopplysninger* tolkes i retning av *sensitive opplysninger* (Solove 2008, 34), og dermed er det en mulighet at dette spørsmålet ikke fanger opp den brede forståelsen av begrepet personopplysninger som lovverket legger til grunn.

At denne variabelen ikke påvirker ønsket om lovregulering kan også tolkes i lys av Helen Nissenbaums teori om *kontekstuell integritet*. Hun skriver at «what people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*» (2010, 2). Det er derfor mulig å hevde at hvis man forstår personopplysninger som *ikke-sensitiv informasjon*, er ikke folks kontrollbehov like sterkt som når spørsmålet omhandler bilder.

Flere undersøkelser (Andrejevic 2009, 50, Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007, Turow 2003) har imidlertid vist at folk ikke begriper omfanget av datainnsamlingen som foregår på nett, og dermed er det ikke nødvendigvis fruktbart å legge for mye vekt på denne tolkningen.

Utdanning påvirker *ikke* ønsket om lovregulering

I tillegg til disse to variablene, som *har* en påvirkningskraft på indeksvariabelen, er det interessant at variabelen *utdanning* ikke påvirker ønsket om lovregulering (tabell 6.4). En viktig årsak til at modellen dagens internett baserer seg på, der personinformasjon byttes mot innhold og tjenester, ikke kan sies å være rettferdig, er den utstrakte kunnskapsmangelen blant forbrukerne (Andrejevic 2009, 50, Jensen, Potts og Jensen 2005, 226, Hoofnagle og King 2008, Turow, Mulligan og Hoofnagle 2007, Turow 2003). En logisk slutning ville derfor vært at høyere utdannelse predikerer et sterkere ønske om lovregulering, all den tid det sannsynliggjør økt kunnskap om praksisen.

Min undersøkelse viser, stikk i strid med denne antakelsen, at de med *lavest* utdannelse uttrykker det sterkeste ønsket om lovregulering. Dette funnet åpner for noen interessante tolkningsmuligheter. Mange personvernerklæringer på nett, altså i praksis kontrakten man skriver når man inngår byttehandelen med personopplysninger, er skrevet på et tørt, juridisk

språk (Sovern 1999, 1099), og i praksis fungerer som juridisk beskyttelse for selskapene snarere enn meningsfull veiledning for forbrukerne (Solove 2004, 82, Pollach 2007, 104, Papacharissi og Fernback 2005, 265). En undersøkelse viste på samme måte at personvernerklæringer ofte er skrevet på et språk som krever minst to års collegeutdannelse, altså høyere utdanning, for å forstå (Antón et al. 2003, 2). At respondentene med lavest utdannelse uttrykker det sterkeste ønsket om lovregulering kan derfor tolkes som at denne gruppen i større grad kjenner på en maktesløshet i møte med internettselskapene.

Det er imidlertid høyst tvilsomt at mennesker med høy utdannelse bruker 40 minutter hver dag på å lese personvernerklæringer på nett, slik en undersøkelse estimerte tiden det faktisk vil ta å gjøre dette (McDonald and Cranor 2008). Derfor er det overraskende at ikke utdanning predikerer et sterkere ønske om lovregulering.

En viktig oppsummerende observasjon er at det generelle ønsket om lovregulering av personopplysninger er sterkt. Frekvensfordelingen i figur 6.9 viser med all tydelighet at tyngdepunktet ligger mot at dette er viktig for befolkningen. Den største gruppen er de med en indeksscore på 12, altså de som har oppgitt *svært viktig* på samtlige variabler som inngår i indeksen. Det er grunn til å hevde at i et velfungerende marked ville ikke ønsket om lovregulering vært så stort. Derfor antyder det generelle høye ønsket om lovregulering at et uregulert marked for kjøp og salg av personopplysninger ikke har støtte i befolkningen, og at dette kan forstås som en konsekvens av de problematiske elementene i markedet jeg har drøftet i teorikapittelet.

6.3 Oppgavens begrensninger

Denne oppgaven baserer seg på et datamateriale samlet inn av Opinion Perduco på oppdrag av Datatilsynet. Som jeg har drøftet i metodekapittelet vil jeg hevde at denne løsningen har gitt meg mulighet til å undersøke tematikken på en mye grundigere måte enn tilfelle hadde vært med et egenprodusert datasett. Det innebærer imidlertid også at jeg ikke har hatt mulighet til å skreddersy spørsmålene i undersøkelsen til akkurat denne oppgavens formål. I tillegg kunne jeg med et eget spørreskjema vært mer konsekvent i hvilke svaralternativer som ble gitt, noe som ville muliggjort et bredere spekter av analysemetoder. Hvis for eksempel aldersvariabelen hadde vært bevart som forholdstallsskala, og ikke kodet om til aldersgrupper, ville det vært mulig å se effekten av denne variabelen enda mer presist.

Jeg vil likevel hevde at muligheten til å undersøke problemstillingene mine ved hjelp av et så omfattende datasett klart veier opp for disse begrensingene. Det er likevel enkelte aspekter ved denne måten å løse oppgaven på som bør diskuteres med hensyn til reliabilitet og validitet.

6.4 Reliabilitet og validitet

En vurdering av denne undersøkelsens reliabilitet vil uunngåelig basere seg på et premiss om at Opinion Perduco er et profesjonelt analysebyrå, med høy kompetanse. Denne oppgaven tar for seg et felt i konstant endring. Teknologien vi i så stor grad avhenger av endres, forbedres, blir kraftigere og mer avansert. Parallelt blir mulighetene for analyse av informasjon trukket fra vår interaksjon med digitale verktøy mer avansert. På samme tid endres kulturelle normer og verdier. De raske endringene på feltet gjør at undersøkelsens reliabilitet bør vurderes i lys av tidspunktet innsamlingen fant sted. Det er, som jeg har diskutert tidligere, viktig å huske på at datamaterialet ble samlet inn i kjølvannet av en av historiens mest omfattende overvåkingsskandaler. Hadde den samme undersøkelsen blitt gjennomført to år tidligere, *før* Snowden, men *rett etter* 22. juli-terroren, er det grunn til å tro at resultatene ville sett annerledes ut. Derfor er det mest hensiktsmessig og tolke funnene fra undersøkelsen som et tidsbilde av befolkningens personvernholdninger i kjølvannet av Snowden-saken.

De to erfaringsvariablene jeg benyttet i undersøkelsen har også egenskaper som det er verdt å diskutere med hensyn til reliabilitet. Som jeg drøftet i analysedelen er det grunn til å hevde at spørsmålet som omhandler *uønsket bildepublisering*, representerer en konkretisering av spørsmålet som spør om *personopplysninger på avveie*. Regresjonsanalysene av disse variablene viste at *personopplysninger på avveie* hadde liten påvirkningskraft, og at denne minsket ytterligere da det ble kontrollert for *uønsket bildepublisering*. På bakgrunn av ulike konseptuelle definisjoner av personvernbegrepet er det sannsynlig at konseptet *personopplysninger på avveie* vurderes på en annen måte enn *uønsket bildepublisering.* Førstnevnte kan forstås som opplysninger som ikke vurderes som verneverdige, selv om det er snakk om personopplysninger. Bilder på den annen side vurderes sannsynligvis som høyst beskyttelsesverdige og private.

Regresjonsanalysene jeg har gjennomført tar utgangspunkt i en indeksvariabel som måler holdninger til lovregulering av flyten av personopplysninger på nett. Et slikt grep øker

undersøkelsens reliabilitet ved at tilfeldige feil får mindre påvirkningskraft (Hjerm og Lindgren 2011, 34). Å benytte en indeks som avhengig variabel i kvantitative analyser øker i tillegg oppgavens validitet. En sammenslåing av flere variabler representerer en bedre operasjonalisering av et teoretisk begrep, noe som innebærer økt definisjonsmessig validitet (Hjerm og Lindgren 2011, 33). Dette metodiske grepet vil jeg derfor hevde har bidratt til å øke oppgavens reliabilitet og validitet.

6.5 Videre forskning

Personvern på internett er et stort og interessant felt, med et bredt spekter av mulige innfallsvinkler og perspektiver. Arbeidet med denne oppgaven har ført meg fra samfunnsvitenskap til juss, økonomi og psykologi. På mange måter har Espen Ytrebergs teltmetafor føltes veldig presis i arbeidet med denne oppgaven: «Hvis man skulle operere med en parallell til et byggverk er medievitenskapen et telt mer enn et tårn. Den er en fleksibel og foreløpig konstruksjon, bygget for folk som stadig er på farten for å kunne overskue det de studerer» (Ytreberg 2008, 8). Det har vært en tøff jobb å velge hvilke steder å skulle feste teltpluggene på denne turen.

Et perspektiv jeg gjerne skulle undersøkt videre er holdninger til personvern i relasjon til dikotomien privatliv/offentlighet. En av grunnene til at dette feltet er så spennende er de konstante endringsprosessene feltet preges av og disse endringene er ikke bare av teknologisk eller samfunnsstrukturell art. Også normer og holdninger til hva som oppfattes som personlig, beskyttelsesverdig og privat er i konstant endring. I tillegg hadde det vært interessant å gjennomføre en studie med utgangspunkt i Helen Nissenbaums *teori om kontekstuell integritet* (2010), hvor en konkret praksis, tjeneste eller teknologi ble undersøkt på bakgrunn av rammeverket hun legger frem. Et ferskt eksempel er Schibstedts ambisjoner om stordataanalyse av personinformasjon fra deres plattformer (Brække 2015). Som jeg har diskutert er det sannsynlig at Snowden-saken har satt sitt preg på hvordan respondentene svarer i en personvernundersøkelse fra 2013. Det hadde derfor vært uhyre interessant å benyttet det samme undersøkelsesopplegget for å lete etter hvor stabile personvernholdningene er.

I arbeidet med oppgaven har jeg åpenbart også valgt bort mulige analyser. Et datamateriale av et slikt omfang som det jeg har tatt utgangspunktet i kunne i prinsippet vært utgangspunkt for

et stort antall masteroppgaver. Én mulighet kunne vært å undersøke hvordan spørsmålet om tillit til ulike organisasjoner og virksomheter som kan sitte på registrerte personopplysninger forholder seg til overgripende personvernholdninger.

Jeg vil likevel hevde at fordelene med å tilnærme seg denne problematikken ved hjelp av kvantitative analyser av et så omfattende datasett, klart veier opp for begrensningene. Jeg vil hevde at det tilhører unntakene at masterstudenter får mulighet til å bryne seg på et tallmateriale av denne typen. Mitt håp er derfor at denne oppgaven kan være et lite bidrag til økt forståelse av det uhyre spennende, men veldig komplekse feltet personvern på internett.

Litteraturliste

Anderson, Janna og Lee Rainie. 2014. "Digital Life in 2025." PEW Research Centre, Lest 11.3.2014. http://www.pewinternet.org/files/2014/03/PIP_Report_Future_of_the_Internet_Predictions_031114.pdf.

Andrejevic, Marc. 2009. "Privacy, Exploitation, and the Digital Enclosure." *Amsterdam Law Forum* 1 (4):47.

Andrejevic, Mark. 2014. "The Infinite Debt of Surveillance in the Digital Economy." I *Media, Surveillance and Identity*, redigert av André Jansson og Miyase Christensen. New York: Peter Lang.

Antón, Annie I. , Julia B. Earp, Davide Bolchini, Qingfeng He, Carlos Jensen og William Stufflebeam. 2003. *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*. Vol. 2015, *theprivacyplace.org*. theprivacyplace.org

Barbaro, Michael. 2006. "A Face Is Exposed for AOL Searcher No. 4417749." *The New York Times*, 9.8.2006. Lest 28.5.2015. http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=2&.

Barnes, Susan B. 2006. "A privacy paradox: Social networking in the United States." *First Monday* 11 (9).

Blaker, Magnus. 2011. "Private Facebook-bilder havnet på pornoside." *teknofil.no*, 2012, Lest 7.12.2011. http://www.teknofil.no/artikler/slettmeg_no_opplever_rekordpaagang/104565

boyd, danah. 2007. "Why youth (heart) social network sites: The role of networked publics in teenage social life." *MacArthur foundation series on digital learning–Youth, identity, and digital media volume*:119-142.

Brække, Jonas. 2015. "Nei til medieovervåking." *Klassekampen*, 2.3.2015. http://www.klassekampen.no/article/20150302/ARTICLE/150309998.

Bygrave, Lee A. 2002. *Data protection law: approaching its rationale, logic and limits*. Vol. 10. Dortrecht: Kluwer.

Christophersen, Knut-Andreas. 2009. *Databehandling og statistisk analyse med SPSS*. 4. utg. Oslo: Unipub.

Datatilsynet. 2013. Personvernundersøkelsen 2013/2014. http://www.datatilsynet.no/verktoy-skjema/Analyser-utredninger/Personvernundersokelser/Personvernundersokelsen-2013-delrapporter/

Datatilsynet. 2014. Appenes informasjon om tilgang til personopplysninger. Lest 23.10.2014. Lest 25.5.2014. http://www.datatilsynet.no/Global/04_planer_rapporter/Appsveip_GPEN_2014.pdf

Foundation, Electronic Frontier. "PATRIOT Act." Electronic Frontier Foundation. Lest 27.5.2015. https://www.eff.org/issues/patriot-act.

Fox, Susannah, Lee Rainie, John Horrigan, Amanda Lenhart, Tom Spooner og Cornelia Carter. 2000. Trust and privacy online: Why Americans want to rewrite the rules. I *The Pew Internet & American Life Project*.

Franzen, Jonathan. 2010. "Imperial Bedroom." I *How to be alone: Essays*. Macmillan.

Froomkin, A Michael. 2000. "The death of privacy?" *Stanford Law Review*:1461-1543.

Færaas, Arild. 2014. "Én av seks nordmenn dropper nettsøk av frykt for konsekvenser." *Aftenposten*, 28.1.2014. Lest 28.5.2015. http://www.aftenposten.no/nyheter/iriks/n-av-seks-nordmenn-dropper-nettsok-av-frykt-for-konsekvenser-7448069.html?hideTopBottom=true.

Gellman, Barton og Laura Poitras. 2013. "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post*, 7.6.2013. Lest 28.5.2015. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Global Privacy Enfocement Network, The. 2013. "Results of the 2013 Global Privacy Enforcement Network Internet Privacy Sweep." Office of the Privacy Commissioner of Canada. Lest 19.3.2015. https://www.priv.gc.ca/media/nr-c/2013/bg_130813_e.asp.

Greenwald, Glenn. 2013. "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'." *The Guardian*, 31.7.2013. Lest 28.5.2015. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Greenwald, Glenn. 2014. *Overvåket : Edward Snowden, NSA og overvåkningsstaten, No place to hide Edward Snowden, the NSA and the U.S. surveillance state*. Oslo: Cappelen Damm.

Grønmo, Sigmund. 2004. *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget

Gulløy, Elisabeth. 1997. Undersøkelse om personvern: holdninger og erfaringer 1997. Statistisk sentralbyrå.

Hamelink, Cees J. 2000. *The ethics of cyberspace*. London: Sage.

Hargittai, Eszter. 2008. "The digital reproduction of inequality." *Social stratification*:936-944.

Hargittai, Eszter, and danah boyd. 2010. "Facebook privacy settings: Who cares?" *First Monday* 15 (8).

Hayes, Andrew F. 2005. *Statistical methods for communication science*. Mahwah, N.J.: Lawrence Erlbaum Associates.

Hjerm, Mikael, Simon Lindgren og Einar Blomgren. 2011. *Introduksjon til samfunnsvitenskapelig analyse*. Oslo: Gyldendal akademisk.

Hoofnagle, Chris Jay og Jennifer King. 2008. What Californians understand about privacy online. SSRN 1262130

Jensen, Carlos, Colin Potts og Christian Jensen. 2005. "Privacy practices of Internet users: self-reports versus observed behavior." *International Journal of Human-Computer Studies* 63 (1):203-227.

Joinson, Adam N. og Carina B. Paine. 2007. "Self-disclosure, privacy and the Internet." I *The Oxford Handbook of Internet Psychology*, redigert av Adam N. Joinson, Katelyn Y.A. McKenna, Tom Postmes og Ulf-Dietrich Reips, 237 - 252. Oxford: Oxford University Press.

Jones, Karen Spärck. 2003. "Privacy: what's different now?" *Interdisciplinary Science Reviews* 28 (4):287-292.

Kerr, Ian R, Jennifer Barrigar, Jacquelyn Burkell og Katie Black. 2009. "Soft surveillance, hard consent." I *Lessons from the identity trail*, redigert av Ian Kerr, Valerie Steeves og Carole Lucock, 5 - 22. Oxford: Oxford University Press.

Kirkpatrick, Marshall. 2010. "Facebook's Zuckerberg Says The Age of Privacy is Over." *readwrite.com*. Lest 2.2.2015 http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.

Lüders, Marika. 2008. "Synlighet og personvern." I *Digitale dilemmaer: nye medieformer, nye utfordringer*, redigert av Eli Skogerbø og Gunn Enli. Oslo: Gyldendal akademisk.

Lyon, David. 2001. *Surveillance society : monitoring everyday life, Issues in society*. Buckingham: Open University Press.

Marx, Gary T. 2006. "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information “Hey Buddy Can You Spare a DNA?”." Lex Electronica, Vol 10:3. Centre de recherche en droit public (CRDP).

Mayer-Schönberger, Viktor og Kenneth Cukier. 2013. *Big data: a revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

McDonald, Aleecia M og Lorrie Faith Cranor. 2008. "The cost of reading privacy policies". *ISJLP* 4:543.

Midtbø, Tor. 2007. *Regresjonsanalyse for samfunnsvitere: med eksempler i SPSS*. Oslo: Universitetsforlaget

Morozov, Evgeny. 2015. "Dyrt å være fattig." *Morgenbladet*, 15.5.2015. Lest 26.5.2015. http://web.retriever-info.com/services/archive/displayPDF?documentId=055126201505153639042 6&serviceId=2.

Nes, Catharina. 2015. "Du er til salgs." *Personvernbloggen*, 22.5.2015. Lest 26.5.2015 https://www.personvernbloggen.no/2015/05/22/du-er-til-salgs/.

Nissenbaum, Helen. 2010. *Privacy in context: technology, policy, and the integrity of social life*. Stanford, Calif: Stanford Law Books.

Norberg, Patricia A, Daniel R Horne og David A Horne. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of Consumer Affairs* 41 (1):100-126.

Papacharissi, Zizi. 2010a. "Privacy as a luxury commodity." *First Monday* 15.

Papacharissi, Zizi. 2010b. *A private sphere: democracy in a digital age, Digital media and society*. Cambridge: Polity.

Papacharissi, Zizi og Jan Fernback. 2005. "Online privacy and consumer protection: An analysis of portal privacy statements." *Journal of Broadcasting and Electronic Media* 49 (3):259-281. doi: 10.1207/s15506878jobem4903_1.

Pengelly, Martin. 2014. "NSA listed Merkel among leaders subject to surveillance – report." *The Guardian*, 29.3.2014. Lest 30.3.2015. http://www.theguardian.com/world/2014/mar/29/nsa-merkel-leaders-surveillance-documents-snowden.

Pollach, Irene. 2007. "What's wrong with online privacy policies?" *Communications of the ACM* 50 (9):103-108. doi: 10.1145/1284621.1284627.

Rainie, Lee, Sara Kiesler, Ruogu Kang og Mary Madden. 2013. *Anonymity, Privacy, and Security Online* pewinternet.org: PEW Research Centre.

Rainie, Lee og Mary Madden. 2015. Americans' Privacy Strategies Post-Snowden. pewinternet.org: PEW Research Centre.

Schartum, Dag Wiese og Lee A. Bygrave. 2011. *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. 2. Utgave. Bergen: Fagbokforlaget

Schauer, Frederick. 1998. "Internet privacy and the public-private distinction. (Symposium: Law and the Internet; Privacy, Jurisdiction, and the Regulation of Free Expression)." *Jurimetrics Journal of Law, Science and Technology* 38 (4):555-564.

Schwartz, Paul M. 1997. "Privacy and the economics of personal health care information." *Tex. L. Rev.* 76:1.

Schwartz, Paul M. 1999. "Privacy and democracy in cyberspace." *Vand. L. Rev.* 52:1607.

Schwartz, Paul M. 2004. "Property, privacy, and personal data." *Harvard Law Review*:2056-2128.

Schwartz, Paul M. 2000. "Internet privacy and the State. (On Privacy and the Internet)." *Connecticut Law Review* 32 (3):815-859.

Selmer, Knut S. og Ragnar Dag Blekeli. 1977. *Data og personvern*. Vol. 6, *Scandinavian university books*. Oslo: Universitetsforlaget.

Shapiro, Andrew L. 1999. *The control revolution: how the Internet is putting individuals in charge and changing the world we know*. New York: PublicAffairs.

Skog, Ole-Jørgen. 2010. *Å forklare sosiale fenomener: en regresjonsbasert tilnærming*. 2. [rev. og utvidet] utgave. 5. opplag Oslo: Gyldendal akademisk.

Smith, Aaron. 2014. *What Internet Users Know about Technology and the Web.* pewresearch.org: PEW Research Centre.

Smith, Dave. 2015. "Google Chairman: "The Internet Will Disappear"." *Business Insider*, 25.1.2015. Lest 10.5.2015. http://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1.

Solove, Daniel J. 2004. *The digital person: technology and privacy in the information age*. New York: New York University Press.

Solove, Daniel J. 2008. *Understanding privacy*. Cambridge, Mass: Harvard University Press.

Sovern, Jeff. 1999. "Opting in, opting out, or no options at all: The fight for control of personal information." *Washington Law Review* 74 (4):1033-1117.

Taylor, Humphrey. 2003. “Most People Are “Privacy Pragmatists” Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits”. Harris Interactive: Harris Interactive.

Tennøe, Tore og Bjørn Erik Thon. 2014. "«Snowden-effekt» kjøler ned norske ytringer." *Aftenposten*, 28.1.2014. Lest 28.5.2015. http://www.aftenposten.no/meninger/kronikker/Snowden-effekt-kjoler-ned-norske-ytringer-7448335.html.

Turow, Joseph. 2003. “Americans & online privacy: The system is broken”. Annenberg Public Policy Center, University of Pennsylvania.

Turow, Joseph, Deirdre K Mulligan og Chris J Hoofnagle. 2007. Research report: Consumers fundamentally misunderstand the online advertising marketplace. I University of Pennsylvania Annenberg School for Communication and UC-Berkeley Samuelson Law Technology and Public Policy Clinic.

Warren, Samuel D. og Louis Dembitz Brandeis. 1890. "The Right to Privacy." *Harvard Law Review Vol. 4, No. 5 (Dec. 15, 1890), 193-220*.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Wikipedia. 2015. "Google Search." [Online Encyclopedia]. Sist oppdatert 19.5.2015. Lest 20.5.2015. http://en.wikipedia.org/wiki/Google_Search.

Ytreberg, Espen. 2008. *Hva er medievitenskap*. Vol. 27, *Hva er*. Oslo: Universitetsforlaget

Østbye, Helge, Knut Helland, Karl Knapskog og Leif Ove Larsen. 2013. *Metodebok for mediefag*. 4. utgave. Bergen: Fagbokforl.

Vedlegg 1: Spørreundersøkelsen

Spørsmål 1

I hvilken grad er du opptatt er du av personvern?

Svaralternativer:

- Svært opptatt av personvern
- Ganske opptatt av personvern
- Lite opptatt av personvern

Spørsmål 2

Har du blitt mer eller mindre opptatt av personvern de siste to-tre årene?

Svaralternativer:

- Mer opptatt enn før
- Like opptatt som før
- Mindre opptatt enn før
- Vet ikke

Spørsmål 3

Er det noen opplysninger om deg eller andre som du mener lovverket særlig bør beskytte mot innsamling og videre bruk? Hvor viktig er det at lovverket beskytter:

- Opplysninger om helsen din
- Dine gener/DNA (opplysninger om arvestoff og sannsynlighet for ulike sykdommer)
- Ditt fødselsnummer/personnummer – 11 siffer
- Din politiske oppfatning
- Din religiøse oppfatning
- Opplysninger om din private økonomi
- Hvilken fagforening du er medlem av

- Opplysninger om steder du har vært og hvor du beveger deg
- Hvilke nettsider du har besøkt/sett på
- Bilder av deg
- Hvem du kommuniserer med på telefon og e-post
- Innholdet i telefonsamtalene og e-posten din
- Hva du har søkt etter på søkemotorer
- Målinger av din effektivitet og tidsbruk på jobb

Svaralternativer:

- Helt uviktig
- Lite viktig
- Litt viktig
- Veldig viktig
- Vet ikke

Spørsmål 5

Under er en liste med tjenester/teknologier som vi ber deg svare om du som privatperson bruker i dag, kunne tenke deg å bruke eller ikke kunne tenke deg å bruke.

- GPS-sporing av barna dine
- GPS-sporing av eldre eller andre familiemedlemmer med spesielt omsorgsbehov
- Kameraovervåkning i eller utenfor eget hjem eller hytte
- Kamera i bil som filmer ut av bilen
- Hjelm- eller actionkamera (f.eks. på sykkel, i slalombakken eller andre steder)
- Opptak av telefonsamtalene dine
- Droner eller radiostyrte helikopter som filmer eller tar bilder fra luften
- Google-briller

Svaralternativer:

- Bruker i dag
- Kunne tenke meg å bruke

- Kunne ikke tenke meg å bruke
- Vet ikke

Spørsmål 12

Har du selv opplevd at personopplysninger om deg er kommet på avveie, eller er blitt misbrukt av andre?

Svaralternativer:

- Ja
- Nei
- Vet ikke

Spørsmål 13

Har du opplevd at noen andre har lagt ut et bilde eller annen informasjon om deg på nett som du ikke ønsket skulle deles?

Svaralternativer:

- Ja
- Nei
- Vet ikke

Spørsmål 28

Hvor enig eller uenig er du i påstandene under?

[Randomiser]

- Offentlige etater, som helsevesen, Nav og politi bør fritt kunne utveksle personopplysninger seg imellom for å avsløre de som utnytter velferdsordninger.
- Det er umulig å ha oversikt over alle som har opplysninger om meg og hvordan opplysningene brukes.
- Bare de som har noe å skjule har behov for personvern.

- Offentlige etater bør fritt kunne utveksle opplysninger om enkeltpersoner for å kunne tilby mest mulige effektive tjenester.
- Hvis jeg publiserer noe på sosiale nettsteder eller åpent på nett, må jeg finne meg i at andre bruker informasjonen til noe helt annet uten å spørre meg.
- Sykehuset, fastlegen min og andre som behandler meg bør fritt kunne utveksle helseopplysningene mine uten å spørre meg først.
- Vi bør tillate sterkere inngripen i privatlivet for å bekjempe kriminalitet.
- Politiet og sikkerhetsmyndigheter bør kunne overvåke og bruke åpen informasjon fra sosiale medier, blogger og andre internettjenester, til forebygging og etterforskning, også om overvåkingen omfatter deg.
- Staten bør lagre en DNA-profil på alle nyfødte til bruk for evtuell senere politietterforskning
- Helseforskere bør kunne bruke opplysninger fra folks pasientjournaler uten den enkeltes samtykke.
- Godt personvern er en forutsetning for et fritt og demokratisk samfunn.

Svaralternativer:

- Helt uenig
- Delvis uenig
- Verken eller
- Delvis enig
- Helt enig
- Vet ikke

Bakgrunnsvariabel

Er du mann eller kvinne?

- Mann (1)
- Kvinne (2)

Bakgrunnsvariabel

Hva er din alder?

Oppgi antall år. Bruk tall.

Bakgrunnsvariabel

Hva er din høyeste fullførte utdanning?

- Grunnskole (1)
- Videregående skole (2)
- Høyskole/universitet inntil 3 år (3)
- Høyskole/universitet over 3 år (4)
- Vet ikke (99)
- Ønsker ikke å oppgi (999)

Vedlegg 2: Faktoranalyse og reliabilitetstest

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,750
Bartlett's Test of Sphericity	Approx. Chi-Square	2355,884
	df	6
	Sig.	,000

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,636	65,902	65,902	2,236	55,888	55,888
2	,626	15,644	81,545			
3	,494	12,341	93,886			
4	,245	6,114	100,000			

Reliabilitetsanalyse:

Reliability Statistics

Cronbach's Alpha	N of Items
,826	4